目　　录

第一章　组合数学的基础……1
§1. 何谓组合数学?……1
§2. 集合……2
§3. 样品……4
§4. 无序选取……6
§5. 二项式系数……10
参考文献……12
第二章　逐步淘汰原理……13
§1. 基本公式……13
§2. 在数论中的应用……15
§3. 更列……17
§4. 积和式……18
参考文献……21
第三章　递推关系……22
§1. 几个初等递推公式……22
§2. 一个计数问题……24
§3. 拉丁长方……27
参考文献……28
第四章　Ramsey 定理……29
§1. 基本定理……29
§2. 若干应用……32
参考文献……35
第五章　相异代表组……36
§1. 基本定理……36
§2. 划分的公共代表组……38
§3. 拉丁长方……39

§4. (0,1)-矩阵 …… 41
§5. 项秩 …… 42
参考文献 …… 45
第六章 (0,1)-矩阵 …… 47
§1. 类 $\mathfrak{A}(R, S)$ …… 47
§2. 对拉丁长方的一个应用 …… 50
§3. 对换 …… 52
§4. 最大项秩 …… 53
§5. 有关问题 …… 58
参考文献 …… 60
第七章 正交拉丁方 …… 61
§1. 存在定理 …… 61
§2. Euler 猜想 …… 65
§3. 有限射影平面 …… 69
§4. 射影平面与拉丁方 …… 71
参考文献 …… 73
第八章 组合设计 …… 74
§1. (b, v, r, k, λ)-组态 …… 74
§2. (v, k, λ)-组态 …… 78
§3. 一个不存在定理 …… 82
§4. 矩阵方程 $AA^T = B$ …… 89
§5. 极值问题 …… 94
参考文献 …… 97
第九章 完备差集 …… 101
§1. 完备差集 …… 101
§2. 乘子定理 …… 104
参考文献 …… 108
记号表 …… 110
人名索引 …… 112
内容索引 …… 114
附：组合矩阵论 …… 120
§1. 引论 …… 120

§2. 关联矩阵………………………………………………………… 121
§3. 积和式………………………………………………………… 123
§4. 对称区组设计………………………………………………… 126
§5. 对称区组设计的近期变体…………………………………… 128
§6. 未定元和关联矩阵…………………………………………… 131
参考文献………………………………………………………… 134

第一章　组合数学的基础

§1. 何谓组合数学？

组合数学，也称作组合分析或组合学，是自古就有的数学分支．据传说，禹在公元前2200多年就观察到神龟背上的幻方

$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}.$$

公元前1100多年，在中国已隐约产生了排列的概念．公元1140年 Rabbi Ben Ezra 似乎已知道从 n 个事物中同时取出 r 个的组合数的公式.古代有关这方面的知识大多联系着数的神秘主义;而近几个世纪来,许多作者又从数学游戏的角度接触这个课题．Bachet的砝码问题，Kirkman 的女生问题和 Euler 的 36 名军官的问题等等,都是这方面有名的例子．这些问题很能推动人们去思索,它们的解答也常常是机智和精巧的.

过去为了娱乐或由于其美学上的魅力而被研究的很多这类问题,现在在纯粹和应用科学上都有重要的价值．不久以前,有限射影平面还只被当作一种组合的珍玩．今天,它在几何基础以及试验的分析和设计中都是基本的．由于离散性问题在现代技术中的极端重要性,过去的趣味数学也被赋予了新的严肃的目的.

更重要的是，现时代为组合数学展现了一系列有吸引力的新问题的广阔范围．这些问题出自抽象代数、拓扑学、数学基础、图论、博弈论、线性规划以及许多其它领域．组合学从来就很驳杂．在我们的时代,这种多样性更是大大地增加了.它的各种各样的问题不能在一个统一的理论中有效地着手解决．以上所述大部分对数论也同样适用．事实上，组合学和数论可以说是姐妹学科．它们在内容上有一定的共同部分,而且彼此真正地互相充实丰富.

组合数学与很多数学分支相交叉，因此很难对它下一个正式的定义．不过大体上可以说，组合数学从事于把一些元素安排成种种集合的研究．这些元素的个数通常是有限的，而这种安排必须服从所论问题提出的限制条件．文献中有两大类问题．在第一类问题中，所论组态（configuration）的存在尚待证实，而我们的研究在于对此作出明确的断言．这类问题称为存在问题．在第二类问题中，已知组态的存在，而我们的研究在于确定组态的数目或作出这些组态的分类．这类问题称为计数问题．本书侧重讨论存在问题，但许多计数问题也时常出现．

或许会认为，第二类问题不过是第一类问题的细致化或明显的推广．是有这种情形．但实际上，如果需要很费劲才能搞清楚组态的存在，则对相应的计数问题几乎一无所知．另一方面，如果计数问题容易处理的话，则相应的存在问题通常是不足道的．

我们用一个初等的例子来解释上述说明．在一个横竖各八格的正方形棋盘上，去掉对角上的两格．现有 31 张骨牌，每张骨牌正好能盖住棋盘的相邻两格．现在的问题是用这 31 张骨牌完全盖住这个去掉了对角上两格的棋盘．在这个问题中，解的存在尚待证实．事实上，我们说这种覆盖是不可能的．设想棋盘上全部 64 个格子黑白相间．如果去掉两个黑格或两个白格，则棋盘上留下的黑白格数不等．但一张骨牌在棋盘上一定同时盖住一黑格和一白格．由于棋盘的对角上的两格必同黑或同白．因此，所要求的覆盖是不可能的．如果对角上两格不去掉，则有许多种方法使 32张骨牌盖住整个棋盘．这时所要讨论的就是确定有多少种不同覆盖方法的计数问题了．

§2. 集合

设 S 是一个元素为 a，b，c，$\cdots$的任意集合．我们用 $s\in S$ 来表示 s 是 S 的一个元素．如果集合 A 的每一个元素都是集合 S 的元素，则称 A 为 S 的一个**子集**，记为 $A\subseteq S$．如果 $A\subseteq S$ 和 $S\subseteq A$ 都成立，则集合 A 与集合 S 等同，记为 $A=S$．如果 $A\subseteq S$，但 $A\neq S$，

则A是S的一个真子集，记为 $A\subset S$． S的所有子集的集合记为$P(S)$．为方便起见，空集或零集$\varnothing$也算成$P(S)$的一个成员．

设S和T是集合M的子集． M中同时满足 $e\in S$和 $e\in T$ 的元素e的集合称为S和T的交，记为 $S\cap T$． 更一般些，如果 T_1，T_2，$\cdots$，T_r 是M的子集，则 $T_1\cap T_2\cap\cdots\cap T_r$ 表示同时满足r个关系 $e\in T_i(i=1,2,\cdots,r)$ 的元素e的集合．如果M的子集S和T没有公共元素，则称S和T不交（disjoint）．关系式 $S\cap T=\varnothing$表示S和T不交． M中满足 $e\in S$ 或 $e\in T$ 的元素e的集合称为S和T的并，记为 $S\cup T$．更一般些，如果 $T_1,T_2,\cdots,T_r$ 是M的子集，则 $T_1\cup T_2\cup\cdots\cup T_r$ 表示元素e的集合，这种e至少满足r个关系 $e\in T_i(i=1,2,\cdots,r)$ 中的一个．M的子集 $T_1,T_2,\cdots,T_r$ 如果满足 $M=T_1\cup T_2\cup\cdots\cup T_r$ 以及 $T_i\cap T_j=\varnothing(i\neq j;\ i,j=1,2,\cdots,r)$，则称 $T_1,T_2,\cdots,T_r$ 组成M的一个划分（partition）． 划分有有序及无序两种． M 的两个有序划分 $M=T_1\cup T_2\cup\cdots\cup T_r$ 和 $M=T_1'\cup T_2'\cup\cdots\cup T_r'$ 相等，表示 $T_i=T_i'(i=1,2,\cdots,r)$ 成立；M的两个无序划分 $M=T_1\cup T_2\cup\cdots\cup T_r$ 和 $M=T_1'\cup T_2'\cup\cdots\cup T_r'$ 相等，表示每一个 T_i 分别等于某一个 T_j'．

只含有限个元素的集合称为有限集．如果一个有限集的元素个数是n，则称它是n个元素的集合． 用这个名词时，我们约定 $n>0$，即不包括零集$\varnothing$． 本书称n个元素的集合为 n-集．于是，一个n-集的一个r-子集，表示一个n个元素的集合中的一个有r个元素的子集．很多数数论证广泛使用下述初等原理．

设S是一个m-集，T是一个n-集．如果 $S\cap T=\varnothing$，则 $S\cup T$ 是一个$(m+n)$-集．此即所谓加法法则．推广的加法法则说：如果 T_i 是 n_i-集 $(i=1,2,\cdots,r)$，并且 $M=T_1\cup T_2\cup\cdots\cup T_r$ 是M的一个划分，则M是一个 $(n_1+n_2+\cdots+n_r)$-集．

设S，T是两个集合． 对 $s\in S$和$t\in T$，记 (s,t) 为一有序对．两个有序对 (s,t) 和 (s^*,t^*) 相等，当且仅当 $s=s^*$，$t=t^*$．所有这种有序对构成的集合称为S和T的积集，记作 $S\times T$． 用

$M(S, T, n)$ 记形如 (s, t) 的有序对的一个集合，其中 s 可以是 S 的任意元素，但每个 $s \in S$ 恰好与 n 个元素 $t \in T$ 相配对. 这里 S 中的不同元素并不一定与 T 的同一个 n-子集的元素相配对. 上述记号表明 T 至少含有 n 个元素. 而且 $M(S, T, n) = S \times T$ 当且仅当 T 是 n-集. 现设 S 是一个 m-集, 则 $M(S, T, n)$ 是一个 (mn)-集. 此即所谓乘法法则. 推广的乘法法则说: 如果 T_1 是 n_1-集，又记 $M_2 = M(T_1, T_2, n_2)$, $M_3 = M(M_2, T_3, n_3)$, $\cdots$, $M_r = M(M_{r-1}, T_r, n_r)$, 则 M_r 是 $(n_1 n_2 \cdots n_r)$-集.

§3. 样品

设 S 是一个集合，并设

$$(a_1, a_2, \cdots, a_r) \tag{3.1}$$

是一个有序 r-组，其中 $a_1, a_2, \cdots, a_r$ 是 S 的元素，但不一定互不相同. 两个这种 r-组 $(a_1, a_2, \cdots, a_r)$ 和 $(a_1^*, a_2^*, \cdots, a_r^*)$ 相等，当且仅当 $a_i = a_i^* (i = 1, 2, \cdots, r)$ 成立. 我们称(3.1)为 S 的一个样品. 样品(3.1)的大小是 r, 故把(3.1)称为 S 的一个 r-样品.

定理 3.1. 一个 n-集的 r-样品的个数为 n^r.

证. 设 S 是 n-集. 本定理是当 $T_1 = T_2 = \cdots = T_r = S$ 和 $n_1 = n_2 = \cdots = n_r = n$ 时推广的乘法法则的特殊情形.

设 S 是 n-集，并设 S 的一个 r-样品 (3.1) 的各个分量 a_i 互不相同，则称这种 r-样品为 n 个元素的一个 r-排列. 对一个 r-排列来讲，必有 $r \leqslant n$. 我们称一个 n-排列为 n 个元素的一个排列.

定理 3.2. n 个元素的 r-排列的个数为

$$P(n, r) = n(n-1)\cdots(n-r+1). \tag{3.2}$$

证. 本定理是当 $T_1 = T_2 = \cdots = T_r = S$, $n_1 = n$, $n_2 = n-1$, $\cdots$, $n_r = n-r+1$ 时推广的乘法法则的特殊情形.

由(3.2)式可知，$P(n, n)$ 是头 n 个正整数的乘积. 称 $P(n, n)$ 为 n-阶乘，记作 $n!$. 即

$$P(n, n) = n! = n(n-1)\cdots 1. \tag{3.3}$$

推论 3.3. n 个元素的排列的个数为 $n!$.

集合 S 到集合 T 中的(单值)映射 α 是一种对应，在这种对应下，每一个 $s\in S$，必有唯一的一个 $t=s\alpha\in T$ 与之相结合. 元素 $s\alpha$ 称为 s 在映射 α 作用下的象. S 到 T 中的两个映射 α 和 β 称为相等，如果 $s\alpha=s\beta$ 对所有 $s\in S$ 成立. 如果每个 $t\in T$ 都是某个 $s\in S$ 的像，映射 α 称为是 S 到 T 上的映射. 如果 S 到 T 上的映射使 S 的不同元素有不同的象，则称这个映射是一一的. 现设 $G(S)$ 是 S 到自身上的所有一一映射的集合. 如果 $\alpha\in G(S)$，$\beta\in G(S)$，则把 $s\in S$ 映为 $(S\alpha)\beta\in S$ 的映射也是一一映射，称它为映射 α 与 β 的乘积. 于是 $G(S)$ 是以上述乘积作为二元合成关系的代数系统，并可验证 $G(S)$ 满足群的公理.

设 S 是一个 n-集，其元素标记为 $1, 2, \cdots, n$，则 $G(S)$ 称为 n 级对称群，记作 S_n. 设 α 是 S_n 的元素，并且 α 把 i 映为 $i\alpha(i=1, 2, \cdots, n)$，则一一映射 α 可以由排列

$$(1\alpha, 2\alpha, \cdots, n\alpha) \tag{3.4}$$

来刻划. 反之，n 个元素的每一个排列实际上是这个 n-集到自身上的一个一一映射. 一个群的元素个数称为它的阶. 我们可以用群论的语言来叙述推论 3.3.

推论 3.4. S_n 的阶是 $n!$.

例. (a) 3 个元素的 2-排列个数是 $P(3, 2)=3\cdot 2=6$. 如果元素标记为 1, 2, 3，这些 2-排列为

$$(1,2),(1,3),(2,1),(2,3),(3,1),(3,2).$$

(b) 用英文字母可以造出 26^5 个 5 个字母的字. 由 5 个不同的字母组成的字的个数为

$$26\cdot 25\cdot 24\cdot 23\cdot 22=7,893,600.$$

(c) S_{100} 约等于 $(9.3326\cdots)10^{157}$，照 Eddington 的估计，宇宙中电子的总数不过 $(136)2^{256}$.

(d) 设 A 是 m 行 n 列的矩阵，其元素都是整数 0 或 1，则这种矩阵共有 2^{mn} 个. 当 $m=n=100$ 时，就有 $2^{10,000}$ 个这种矩阵.

§4. 无序选取

设 S 是一个集合，并设

$$\{a_1, a_2, \cdots, a_r\} \tag{4.1}$$

是一个无序 r-组，其中 $a_1, a_2, \cdots, a_r$ 是 S 的元素，但不一定互不相同．一个元素在无序 r-组 (4.1) 中出现的次数称为此元素在 (4.1) 中的重数．两个这种无序 r-组 $\{a_1, a_2, \cdots, a_r\}$ 和 $\{a_1^*, a_2^*, \cdots, a_r^*\}$ 相等，当且仅当每个元素在这两个无序 r-组中的重数相同．我们称(4.1)式为 S 的一个无序选取．无序选取 (4.1)式的大小是 r，故称(4.1)式为 S 的一个 r-选取．如果在(4.1)式中，每个元素的重数都是 1，则此 r-选取是 S 的一个r-子集．一个 n-集的 r-子集也称为 n 个元素的一个 r-组合．

当 n 是正整数时，(3.3) 式断言

$$n! = P(n, n). \tag{4.2}$$

为方便起见，可以规定

$$0! = 1, \tag{4.3}$$

于是对每个正整数 n，都有

$$n! = n(n-1)!. \tag{4.4}$$

现设 n 和 r 为正整数，并定义

$$\begin{aligned} C(n, r) &= \binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!}, \\ C(n, 0) &= \binom{n}{0} = 1, \\ C(0, r) &= \binom{0}{r} = 0, \\ C(0, 0) &= \binom{0}{0} = 1, \end{aligned} \tag{4.5}$$

再规定当 $r > n$ 时，$C(n, r) = 0$，则 (4.5) 式对所有非负整数 n 和 r 都定义了 $C(n, r)$．这说明当 n 固定时，$C(n, r)$ 只取有限个不同的值．由(4.5)式所定义的数 $C(n, r)$ 正是熟知的二项系数．

它们在计数问题中非常重要.

定理 4.1. 一个 n-集的 r-子集的个数为 $\binom{n}{r}$.

证. 由定理 3.2 可知, n 个元素的 r-排列的个数为 $P(n, r)$. 每个 r-排列可以用 $r!$ 种方法安排次序. 如果不计次序, 即得不同的 r-子集的个数为

$$C(n, r) = \frac{P(n, r)}{r!}. \tag{4.6}$$

设 S 是一个 n-集, 又设 $P(S)$ 表示 n-集 S 的所有子集的集合. 设 T 表示元素为整数 0, 1 的一个 2-集的所有 n-样品的集合, 则有 $P(S)$ 到 T 上的一个自然的一一映射: 设 $X = \{a_{i_1}, a_{i_2}, \cdots, a_{i_r}\} \in P(S)$, X 的像是一个 n-样品, 这个 n-样品的第 $i_1, i_2, \cdots, i_r$ 个分量为 1, 其余 $n - r$ 个分量都为 0. 现在我们可以用定理 4.1 来数出 $P(S)$ 的元素个数, 又可以用定理 3.1 来数出 T 的元素个数. 它们应当相等, 故得

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n. \tag{4.7}$$

当然 (4.7) 不过是一个初等恒等式. 但它的上述证明方法说明了一种在很多组合研究中有效的数数论证法.

定理 4.2. 一个 n-集的 r-选取的个数为

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{r}. \tag{4.8}$$

证. 取 n-集 S 为由正整数 $1, 2, \cdots, n$ 所组成的集合 S', 则 S' 的每个 r-选取可以表为

$$\{a_1, a_2, \cdots, a_r\}, \tag{4.9}$$

其中

$$a_1 \leqslant a_2 \leqslant \cdots \leqslant a_r. \tag{4.10}$$

令 S^* 为正整数 $1, 2, \cdots, n + r - 1$ 组成的 $(n + r - 1)$-集, 则

$$\{a_1 + 0, a_2 + 1, \cdots, a_r + r - 1\} \tag{4.11}$$

是 S^* 的一个 r-子集. 而且对应

$$\{a_1, a_2, \cdots, a_r\} \longleftrightarrow \{a_1 + 0, a_2 + 1, \cdots, a_r + r - 1\} \quad (4.12)$$

是从 S' 的所有 r-选取到 S^* 的所有 r-子集上的一一映射. 由定理 4.1 可知, S^* 的 r-子集个数为

$$\binom{n+r-1}{r}.$$

故定理得证.

设

$$S = T_1 \cup T_2 \cup \cdots \cup T_k \quad (4.13)$$

是 n-集 S 的一个划分,这里 T_i 是 r_i-子集 $(i = 1, 2, \cdots, k)$, 则

$$n = r_1 + r_2 + \cdots + r_k. \quad (4.14)$$

我们称划分(4.13)为 S 的一个 $(r_1, r_2, \cdots, r_k)$-划分.

定理 4.3. 一个 n-集的有序 $(r_1, r_2, \cdots, r_k)$-划分的个数为

$$\frac{n!}{r_1! r_2! \cdots r_k!}. \quad (4.15)$$

证. 根据定理 4.1 以及推广的乘法法则, 可知一个 n-集的有序 $(r_1, r_2, \cdots, r_k)$-划分的个数等于

$$\binom{n}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_1-\cdots-r_k}{r_k} = \frac{n!}{r_1! r_2! \cdots r_k!}. \quad (4.16)$$

数(4.15)是所谓的多项式系数.从定理 4.3 可以推得 n-集的有序$(1,1,\cdots,1)$-划分的个数为 $n!$,这时定理 4.3 即化为推论 3.3. n-集的有序 $(r, n-r)$-划分个数为

$$\frac{n!}{r!(n-r)!},$$

这时定理 4.3 即化为定理 4.1.

定理 4.3 中的多项式系数还有另一种很有用的组合解释. 设 S 是元素为 $a_1, a_2, \cdots, a_k$ 的 k-集,并设

$$n = r_1 + r_2 + \cdots + r_k, \quad (4.17)$$

其中 r_i 都是正整数. 设 $(a_{i_1}, a_{i_2}, \cdots, a_{i_n})$ 是 S 的一个 n-样品, 其中 a_i 正好出现 r_i 次 $(i = 1, 2, \cdots, k)$. 记 T 为所有这种样品的集合,则 T 的元素个数是

$$\frac{n!}{r_1!r_2!\cdots r_k!}. \tag{4.18}$$

因为在每个样品中，r_1 个 a_1 可以换成 r_1 个彼此不同并与样品中其它元素也不同的元素．这 r_1 个新元素可以按 $r_1!$ 种方法在原来都是 a_1 的位置上排列，故每个样品产生出 $r_1!$ 个新样品．在如此产生的新样品的集合中，同样可把每个样品中的 r_2 个 a_2 换成 r_2 个彼此不同并与样品中其它元素也不同的元素，这时每个样品产生出 $r_2!$ 个新样品．继续这种替换手续，最终得到 n 个元素的 $n!$ 个排列．所以 T 的元素个数正如（4.18）所示．

例．(a) 从一副 52 张扑克牌中任取 13 张得一手牌，在每一手牌中不考虑这 13 张牌的次序，则总共有

$$\binom{52}{13}=635,013,559,600$$

手不同的牌．

(b) 把一副 52 张扑克牌分给 4 个人，每人得 13 张，则总共有

$$\frac{52!}{(13!)^4}=(5.3645\cdots)10^{28}$$

种不同的牌局．

(c) 由 4 个 a，4 个 b，2 个 c 和 2 个 d 这 12 个字母能组成

$$\frac{12!}{4!4!2!2!}=207,900$$

个具有 12 个字母的字．

(d) 用字母 a，b，c 组成 5 个字母的字，每个字中 a 至多出现 2 次，b 至多 1 次，c 至多 3 次．这种字的个数为

$$\frac{5!}{2!0!3!}+\frac{5!}{2!1!2!}+\frac{5!}{1!1!3!}=60.$$

(e) 将 r 个骰子掷一次，可以看成一个 6-集的 r-选取．所以总共可能掷出

$$\binom{r+5}{5}=\binom{r+5}{r}$$

种不同结果.

§5. 二项式系数

设 n 和 r 是正整数,则

$$\binom{n}{r}=\binom{n-1}{r}+\binom{n-1}{r-1}. \tag{5.1}$$

公式(5.1)是定义(4.5)的直接推论,它提供了关于二项式系数的一个基本递推公式. §4 的推论告诉我们二项式系数是整数,现在直接用归纳法来证明这个断言. 当 $n=0$ 或 $r=0$ 时,由(4.5)易知结论为真. 如果 n 和 r 都是正整数,由归纳法假设已知(5.1)式右边两项都是整数,所以左边也必为整数. 这个结论可以更醒目地重述为: r 个相继的正整数的乘积可被 $r!$ 整除.

我们把只能被自身以及 1 整除的正整数称作素数.

定理 5.1. 如果 p 是素数,则

$$\binom{p}{1}, \binom{p}{2},\cdots,\binom{p}{p-1} \tag{5.2}$$

都能被 p 整除.

证. 设 r 是区间 $1\leqslant r\leqslant p-1$ 中的一个整数, 则 $r!$ 可整除

$$p(p-1)\cdots(p-r+1). \tag{5.3}$$

但 $r!$ 与 p 互素,因而 $r!$ 可整除

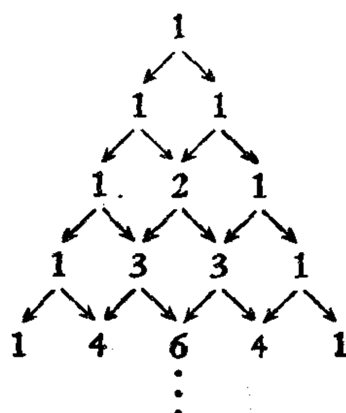
$$(p-1)(p-2)\cdots(p-r+1). \tag{5.4}$$

所以

$$\binom{p}{r}=p\frac{(p-1)(p-2)\cdots(p-r+1)}{r!} \tag{5.5}$$

能被 p 整除.

公式 (5.1) 指出了一种计算二项式系数的有效程序. 它可以图示如下



$$(5.6)$$

上图就是所谓杨辉三角形[1]. 在(5.6)中，我们把箭头当作一个单向路. 如果有可能从一个二项式系数 P 出发，顺着首尾相继的单向路而止于另一个二项式系数 Q,则称 P 和 Q 可用单向路径相连. 用 I 来记最顶端的那个1，则 I 和 P 可用多种单向路径相连. 而二项式系数 P 正好等于这些不同路径的个数. 杨辉三角形的这种有趣特色，是(5.1)式所产生的结构的一个内在性质. 杨辉三角形中水平行上的对称性和增减变化，是下列关系的推论：

$$\binom{n}{r}=\binom{n}{n-r} \qquad (0\leqslant r\leqslant n), \tag{5.7}$$

$$\binom{2n}{0}<\binom{2n}{1}<\cdots<\binom{2n}{n}, \tag{5.8}$$

$$\binom{2n-1}{0}<\binom{2n-1}{1}<\cdots<\binom{2n-1}{n-1}=\binom{2n-1}{n}. \tag{5.9}$$

设 n 是正整数，则有

$$(x+y)^n=\binom{n}{0}x^n+\binom{n}{1}x^{n-1}y+\cdots+\binom{n}{n}y^n. \tag{5.10}$$

这个代数恒等式就是著名的二项式定理. 我们用§4的想法给(5.10)一个证明. 设 S 是由符号

$$(x+y)_1,(x+y)_2,\cdots,(x+y)_n \tag{5.11}$$

组成的 n-集，则对于 $r>0$，展开式 $(x+y)^n$ 中 $x^{n-r}y^r$ 项的系数等于 S 的 r-子集的个数. 而由定理4.1可知，后者等于

1) 原书称为 Pascal 三角形. ——译者注

$$\binom{n}{r}, \tag{5.12}$$

于是 (5.10) 成立.

许多有关二项式系数的恒等式都是 (5.1) 和 (5.10) 的简单推论. 公式 (5.1) 可作为用归纳法来证明恒等式的典型例子. 展开式 (5.10) 可以形式地处理, 从而是二项式系数之间很多关系式的一个直接来源. 例如, 若在(5.10)中取 $x = y = 1$, 则得

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n. \tag{5.13}$$

另外, 如取 $x = 1$, $y = -1$, 则得

$$\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n\binom{n}{n} = 0. \tag{5.14}$$

下列恒等式是文献中常见的典型, 它们都能用初等方法导出.

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}, \tag{5.15}$$

$$\sum_{k=1}^{n} k\binom{n}{k} = n \cdot 2^{n-1}, \tag{5.16}$$

$$\sum_{k=1}^{n} k^2\binom{n}{k} = n(n+1) \cdot 2^{n-2}, \tag{5.17}$$

$$\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}\binom{n}{k} = 1 + \frac{1}{2} + \cdots + \frac{1}{n}. \tag{5.18}$$

参 考 文 献

在 Dickson[1] 的第九章中, 讨论了很多二项式系数及多项式系数的可除性.

[1] L. E. Dickson, History of the Theory of Numbers, Vol. 1, New York, Chelsea, 1952.

[2] W. Feller, Probability Theory and Its Applications, Vol. 1, New York, Wiley, 1950. (中译本: 概率论及其应用(上册), 科学出版社, 1964.)

[3] E. Netto, Lehrbuch der Combinatorik, Leipzig, Teubner, 2nd edition, 1927, reprinted by Chelsea.

[4] J. Riordan, An Introduction to Combinatorial Analysis, New York, Wiley, 1958.

第二章　逐步淘汰原理[1)]

§1. 基本公式

设 S 是一个 n-集，F 是一个域．对每个 $a\in S$，指派唯一的一个 $w(a)\in F$，称 $w(a)$ 为 a 的权．这里对域 F 以及在 F 中如何指派权 $w(a)$ 没有任何限制．不过在所需讨论的组合问题中，通常都能以某种自然的方式来指派权．在很多问题中，对每个 $a\in S$ 都指派正整数 1 为权 $w(a)$．现设

$$P_1, P_2, \cdots, P_N \tag{1.1}$$

是与 S 的元素有关的 N 个性质，P 是元素为(1.1)的 N-集．对 P 的一个 r-子集

$$\{P_{i_1}, P_{i_2}, \cdots, P_{i_r}\}, \tag{1.2}$$

令

$$W(P_{i_1}, P_{i_2}, \cdots, P_{i_r}) \tag{1.3}$$

等于 S 中同时具有这 r 个性质 $P_{i_1}, P_{i_2}, \cdots, P_{i_r}$ 的元素的权的和．如果 S 中没有元素同时具有这 r 个性质，则规定(1.3)等于 0．再以

$$W(r)=\sum W(P_{i_1}, P_{i_2}, \cdots, P_{i_r}) \tag{1.4}$$

表示所有量 (1.3) 之和，其中和式取遍 P 的 r-子集．当 $r=0$ 时，规定 $W(0)$ 等于 S 中所有元素的权的和．现在我们可以提出基本的逐步淘汰公式．

定理 1.1.　令 $E(m)$ 表示 S 中正好具有(1.1)中的 m 个性质的元素的权的和，则以下公式成立：

$$E(m)=W(m)-\binom{m+1}{m}W(m+1)+\binom{m+2}{m}W(m+2)-\cdots+(-1)^{N-m}\binom{N}{m}W(N). \tag{1.5}$$

---

1) 或称容斥原理．——译者注

证. 设 $a \in S$, 且 a 正好具有 (1.1) 中的 t 个性质. 如果 $t < m$, 则 a 对(1.5)式右边没有贡献. 如果 $t = m$, 则 a 对(1.5) 式右边贡献 $w(a)$. 而当 $t > m$ 时, a 对 (1.5) 式右边的贡献等于

$$\left[\binom{t}{m} - \binom{m+1}{m}\binom{t}{m+1} + \binom{m+2}{m}\binom{t}{m+2} - \cdots + (-1)^{t-m}\binom{t}{m}\binom{t}{t}\right] w(a). \tag{1.6}$$

但是

$$\binom{k}{m}\binom{t}{k} = \binom{t}{m}\binom{t-m}{t-k} \quad (m \leqslant k \leqslant t), \tag{1.7}$$

因此 (1.6) 式可以化为

$$\binom{t}{m}\left[\binom{t-m}{t-m} - \binom{t-m}{t-(m+1)} + \binom{t-m}{t-(m+2)} - \cdots + (-1)^{t-m}\binom{t-m}{t-t}\right] w(a). \tag{1.8}$$

由第一章 (5.14) 式可知,(1.8) 式中方括号内的和式等于 0. 于是当 $t > m$ 时, a 对(1.5)式右边同样没有贡献. 这就说明,(1.5) 式右边等于 S 中正好具有(1.1)式中的 m 个性质的元素的权的和.

定理 1.2. 令 $E(0)$ 表示 S 中不具有(1.1)中的任何性质的元素的权的和,则以下公式成立:

$$E(0) = W(0) - W(1) + W(2) - \cdots + (-1)^N W(N). \tag{1.9}$$

证. 这是当 $m = 0$ 时定理 1.1 的特殊情形.

如果对每个 $a \in S$, 指定的权 $w(a)$ 都等于正整数 1,则一些元素的权的和就等于这些元素的个数. 这时 $W(0) = n$, $E(0)$ 表示 S 中不具有 (1.1) 式中的任何性质的元素的个数. 在这种特殊情形下,(1.9) 式称为**筛式**. 它被认为是 da Silva 和 Sylvester 的发明. 实际上筛式是很老的,Bernoulli 家族可能已经知道了这种类型的公式.本章其余各节都用来讨论定理 1.1 的种种应用.

§2. 在数论中的应用

本节我们用筛式 (1.9) 来讨论几个初等数论的问题.

如果 x 是 $\geqslant 0$ 的实数,我们用

$$[x] \tag{2.1}$$

记 $\leqslant x$ 的最大整数. 对两个不全为 0 的整数 a 和 b, 我们用

$$(a, b) \tag{2.2}$$

记 a 和 b 的最大公约数.因此 $(a, b) = 1$ 表示 a 和 b 互素.

如果 a 能整除 b, 则记为

$$a \mid b. \tag{2.3}$$

如果 a 不能整除 b, 则记为

$$a \nmid b. \tag{2.4}$$

定理 2.1. 设 n 是正整数,且 $a_1, a_2, \cdots, a_N$ 是 N 个两两互素的正整数,则满足

$$0 < k \leqslant n, \quad a_i \nmid k \qquad (i = 1, 2, \cdots, N) \tag{2.5}$$

的整数 k 的个数等于

$$n - \sum_{1 \leqslant i \leqslant N} \left[\frac{n}{a_i}\right] + \sum_{1 \leqslant i < j \leqslant N} \left[\frac{n}{a_i a_j}\right] - \cdots + (-1)^N \left[\frac{n}{a_1 a_2 \cdots a_N}\right]. \tag{2.6}$$

证. 记正整数 $1, 2 \cdots, n$ 所组成的 n-集为 S. P_i 表示 S 中元素能被 $a_i (i = 1, 2, \cdots, N)$ 整除的性质.

由于 a_i 两两互素,因此在筛式中表示式

$$W(P_{i_1}, P_{i_2}, \cdots, P_{i_r}) \tag{2.7}$$

是满足关系

$$0 < k \leqslant n, \quad a_{i_1} a_{i_2} \cdots a_{i_r} \mid k \tag{2.8}$$

的整数 k 的个数. 而它等于

$$\left[\frac{n}{a_{i_1} a_{i_2} \cdots a_{i_r}}\right]. \tag{2.9}$$

故由筛式 (1.9) 可推得(2.6).

定义正整数 n 的 Euler φ-函数为满足

$$0 < k \leqslant n, \quad (k,n) = 1 \tag{2.10}$$

的整数 k 的个数.

定理 2.2. 设 n 是正整数，则有

$$\varphi(n) = n \prod_p \left(1 - \frac{1}{p}\right), \tag{2.11}$$

其中乘积遍取 n 的所有素因子 p.

证. 在定理 2.1 中，把 a_i 取为 p_i，并假定 $p_1, p_2, \cdots, p_N$ 是 n 的全部素因子，则由(2.6)可得

$$\varphi(n) = n - \sum_{1 \leqslant i \leqslant N} \frac{n}{p_i} + \sum_{1 \leqslant i < j \leqslant N} \frac{n}{p_i p_j} - \cdots + (-1)^N \frac{n}{p_1 p_2 \cdots p_N}. \tag{2.12}$$

此式等价于 (2.11) 式.

定义正整数 n 的 Möbius 函数 $\mu(n)$ 如下:

$$\begin{cases} \mu(1) = 1, & \\ \mu(n) = 0, & \text{如果 } n \text{ 能被某素数的平方整除}, \\ \mu(p_1 p_2 \cdots p_k) = (-1)^k, & \text{如果素数 } p_1, p_2, \cdots, p_k \text{ 互不相同}. \end{cases} \tag{2.13}$$

用 Möbius 函数可把 (2.12) 式表成更精练的形式:

$$\varphi(n) = n \sum_d \frac{\mu(d)}{d}. \tag{2.14}$$

在(2.14)中，和式遍取 n 的所有正因子 d.

设 n 是正整数. 如果已知 $\leqslant \sqrt{n}$ 的全部素数，则可按下面的方法找出 $\leqslant n$ 的全部素数. 先把整数排成序列

$$2, 3, \cdots, n. \tag{2.15}$$

然后在序列 (2.15) 中划去所有能被 2 除尽的数，再划去所有能被 3 除尽的数，再划去能被 5 除尽的数，一直到划去能被 q 除尽的数，这里 q 是 $\leqslant \sqrt{n}$ 的最大素数. 最后留下来的就是所有 $> \sqrt{n}$ 和 $\leqslant n$ 的素数. 因为留下来的每一个数既不可能有 $\leqslant \sqrt{n}$ 的素因子，又不可能是两个 $> \sqrt{n}$ 的数的乘积. 这种找出 $\leqslant n$ 的全部素

数的有效方法称为 Eratosthenes 的筛法.

现设 x 是一个正实数，用 $\pi(x)$ 记 $\leqslant x$ 的素数个数. 对(2.15)用 Eratosthenes 的筛法后，正好还留下

$$\pi(n)-\pi(\sqrt{n}) \tag{2.16}$$

个整数. 还可以用另一种方法来计算这些留下的整数的个数. 在定理 2.1 中，把 a_i 取为 q_i，并假定 $q_1, q_2, \cdots, q_N$ 是 $\leqslant\sqrt{n}$ 的全部素数. 由定理 2.1 可知，所求的数等于

$$\begin{aligned}-1+n-\sum_{1\leqslant i\leqslant N}\left[\frac{n}{q_i}\right]+\sum_{1\leqslant i<j\leqslant N}\left[\frac{n}{q_iq_j}\right]\\ -\cdots+(-1)^N\left[\frac{n}{q_1q_2\cdots q_N}\right].\end{aligned} \tag{2.17}$$

于是可得

$$\pi(n)-\pi(\sqrt{n})=-1+\sum_{d}\mu(d)\left[\frac{n}{d}\right]. \tag{2.18}$$

在 (2.18) 式中，和式遍取乘积 $q_1q_2\cdots q_N$ 的正因子 d，这里 q_1，$q_2,\cdots,q_N$ 是 $\leqslant\sqrt{n}$ 的全部素数.

§ 3. 更列

设

$$(a_1, a_2, \cdots, a_n) \tag{3.1}$$

是元素 1, 2, …, n 的一个排列. 如果 $a_i\neq i(i=1,2,\cdots,n)$，则称这种排列 (3.1) 为一个更列 (derangement). 也就是说，在一个更列中，没有元素在它的自然位置上. 通常以它的法文名称“相遇问题” (le problème des recontres) 为人所知的 Montmort 问题就是要确定更列的个数. 现记更列(3.1)的个数为 D_n. 我们不难用筛式来求得 D_n.

设 S 是 $n!$ 个排列 (3.1) 的集合. 如果在一个排列 (3.1) 中有 $a_i=i$，则称此排列具有性质 $P_i(i=1,2,\cdots,n)$. 易知有

$$W(P_{i_1}, P_{i_2}, \cdots, P_{i_r})=(n-r)! \tag{3.2}$$

和

$$W(r)=\binom{n}{r}(n-r)!=\frac{n!}{r!}. \tag{3.3}$$

于是由筛式可得 D_n 的下列公式:

$$D_n=n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!}\right). \tag{3.4}$$

(3.4)式使人联想起 e^{-1} 的级数表示

$$e^{-1}=1-\frac{1}{1!}+\frac{1}{2!}-\cdots. \tag{3.5}$$

因此我们又可将 (3.5) 式写成

$$e^{-1}=\frac{D_n}{n!}+(-1)^{n+1}\frac{1}{(n+1)!}\pm\cdots, \tag{3.6}$$

它说明 $\frac{D_n}{n!}$ 和 e^{-1} 相差小于 $\frac{1}{(n+1)!}$. 因此, $n!e^{-1}$ 是 D_n 的很好的近似值.

(3.4)式有一些有趣的应用. 例如, 设想有 n 个客人去参加一个晚会. 他们都把帽子放在寄存处,后来帽子混起来了,而且随机地归还给客人们, 则每个客人都没有得到自己的帽子的概率等于 $D_n/n!$. 这个例子有多种情况, 但殊堪注意的是, 无论是有 10 个客人还是有 10,000 个客人,所论概率实际上都可认为等于 e^{-1}. 下面一个问题稍稍严肃一些.假如要在国际象棋的棋盘上放 8 个车,使它们都不在白色对角线上,而且彼此不能相吃,问共有多少种摆法? 不难得到答案是 $D_8=14,833$.

§4. 积和式

以下假定读者了解一些矩阵的初等性质. 我们在这里引入一组全书通用的记号和术语. 设 S 是一个集合. 如下的 m 行 n 列的组态

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \tag{4.1}$$

称为一个 S 上的长方阵列. A 中位于第 i 行和第 j 列处的元素 a_{ij} 必须属于 S，但对集合 S 没有任何限制. 我们说 a_{ij} 在 A 的 (i, j) 位置上. 当我们想强调 A 有 m 行 n 列时，我们就称 A 为 $m \times n$ 阵列，或称 A 是 $m \times n$ 型的. 如果 $m = n$，则 A 为 n 阶方阵列. 如果在 A 中去掉 $m-r$ 行和 $n-s$ 列，则留下的 $r \times s$ 长方阵列称为 A 的一个子阵列. 两个 $m \times n$ 阵列相等，规定为它们在所有 (i, j) 位置上的相应元素相等 $(i = 1, 2, \cdots, m; j = 1, 2, \cdots, n)$. 在一定的意义上，阵列(4.1)不过是给定集合 S 的一个 mn-样品. 但从另一方面看，$1 \times n$ 阵列可以当作 n-样品，从而阵列 (4.1) 是样品概念的自然推广. 我们可以把阵列 (4.1) 简记为

$$A = [a_{ij}] \qquad (i = 1, 2, \cdots, m; j = 1, 2, \cdots, n). \tag{4.2}$$

令 $e = \min(m, n)$，则所有在 (i, i) 位置上的元素构成 A 的主对角线，这里 $i = 1, 2, \cdots, e$. A 对它的主对角线作反射后所得的 $n \times m$ 阵列称为 A 的转置，记为 A^T. A^T 在 (i, j) 位置上的元素是 $a_{ji} (i = 1, 2, \cdots, n; j = 1, 2, \cdots, m)$. 如果 $A = A^T$，称 A 是对称的.

现设 S 是域，则长方阵列就是一个矩阵. $m \times n$ 矩阵的加法以及数量乘法按通常定义，而且元素属于 F 的所有 $m \times n$ 矩阵构成一个域 F 上的 mn 维向量空间. $m \times n$ 矩阵按熟知的行列相乘法则还可以和 $n \times t$ 矩阵相乘，其乘积是 $m \times t$ 矩阵. 如果 A 是 $m \times n$ 矩阵，则一定有乘积 AA^T 和 A^TA，它们分别是 m 阶和 n 阶对称方阵.

现设 $A = [a_{ij}]$ 是 $m \times n$ 矩阵，而且 $m \leqslant n$. 我们作和式

$$\operatorname{per}(A) = \sum a_{1i_1} a_{2i_2} \cdots a_{mi_m}. \tag{4.3}$$

在(4.3)式右边，和式遍取 1, 2, $\cdots$, n 的所有 m-排列 $(i_1, i_2, \cdots, i_m)$. 我们称 (4.3) 式为 A 的积和式(permanent). 它作为矩阵 A 的数量函数，在与一些计数问题和极值问题有关的组合数学的文献中经常出现. 现在我们讨论 $\operatorname{per}(A)$ 的某些表面上的性质. 首先，在 A 的行(或列)的任意置换下，$\operatorname{per}(A)$ 不变. 另外，如用 $a \in F$ 乘 A 的某一行，则 $\operatorname{per}(A)$ 变为 $a \cdot \operatorname{per}(A)$. 我们再讨论一种重要

情形，即 A 是方阵的情形。这时，$\mathrm{per}(A)$ 在转置下不变，即有

$$\mathrm{per}(A) = \mathrm{per}(A^T). \tag{4.4}$$

对方阵 A 来说，$\mathrm{per}(A)$ 的展开式和 A 的行列式 $\det(A)$ 的展开式的各项相同，只是有一半项相差因子 -1。这就提出了把丰富的 $\det(A)$ 的理论类推为计算 $\mathrm{per}(A)$ 的方法的可能性。事实上，行列式的有些法则确实可以类推。例如，对积和式，就有与行列式的 Laplace 展开完全类似的结果。但行列式的乘法定理

$$\det(AB) = \det(A)\det(B) \tag{4.5}$$

对积和式就不成立。另外，如用 $a \in F$ 乘 A 的某一行后再加到另一行上，$\det(A)$ 不变，但 $\mathrm{per}(A)$ 要改变。这些对计算 $\mathrm{per}(A)$ 都是极大的妨碍。所以往往有许多方阵的行列式的计算很简单，但很难求出它们的积和式。现在叙述一种计算 $\mathrm{per}(A)$ 的方法。

定理 4.1. 设 A 是 $m \times n$ 矩阵，$m \leqslant n$。把 A 的某 r 列改成零后所得的 $m \times n$ 矩阵记为 A_r，并记这个 A_r 的 m 个行的行和的乘积为 $S(A_r)$。再令 $\sum S(A_r)$ 为所有可能取得的 A_r 的 $S(A_r)$ 之和，则

$$\begin{aligned}\mathrm{per}(A) = \sum S(A_{n-m}) &- \binom{n-m+1}{1} \sum S(A_{n-m+1}) \\ &+ \binom{n-m+2}{2} S(A_{n-m+2}) - \cdots \\ &+ (-1)^{m-1} \binom{n-1}{m-1} \sum S(A_{n-1}).\end{aligned} \tag{4.6}$$

证. 设 S 是正整数 $1, 2, \cdots, n$ 的所有 m-样品

$$(j_1, j_2, \cdots, j_m) \tag{4.7}$$

的集合。令样品(4.7)的权为

$$a_{1j_1} a_{2j_2} \cdots a_{mj_m}. \tag{4.8}$$

S 的元素(4.7)不包含整数 $i(i = 1, 2, \cdots, n)$ 的性质记为 P_i。如果 A_r 是在 A 中把第 $i_1, i_2, \cdots, i_r$ 列改成零后所得的矩阵，则

$$W(P_{i_1}, P_{i_2}, \cdots, P_{i_r}) = S(A_r), \tag{4.9}$$

从而

$$W(r) = \sum S(A_r). \tag{4.10}$$

函数 per(A) 的值等于 S 中正好具有 n-m 个性质 $P_i(i=1, 2, \cdots, n)$ 的元素的权的和．由定理 1.1 即得(4.6)．

推论 4.2. 设 A 为 n 阶方阵，则

$$\begin{aligned}\operatorname{per}(A) = S(A) - \sum S(A_1) + \sum S(A_2) - \cdots \\ + (-1)^{n-1}\sum S(A_{n-1}).\end{aligned} \tag{4.11}$$

证．这是定理 4.1 当 $m = n$ 时的情形．

我们把元素都是整数 0 或 1 的矩阵称作 (0, 1)-矩阵．全部 2^{mn} 个(0,1)-矩阵在组合学中很重要，它们在今后的讨论中将起主导作用．现在仅就与积和式有关的几个很特殊的(0,1)-矩阵稍作说明．

设 I 是 n 阶单位方阵，J 是所有元素都等于 1 的 n 阶方阵．显然有

$$\operatorname{per}(J) = n! \tag{4.12}$$

和

$$\operatorname{per}(J - I) = D_n. \tag{4.13}$$

从(4.11)和(4.12)式可得恒等式

$$n! = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n - r)^n. \tag{4.14}$$

又从 (4.11) 和 (4.13) 式可得更列数的另一个公式，即

$$D_n = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n - r)^r (n - r - 1)^{n-r}. \tag{4.15}$$

参 考 文 献

[1] W. Feller, 同第一章参考文献[2].

[2] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford Uuiv. Press, 3rd edition, 1954.

[3] T. Nagell, Introduction to Number Theory, New York, Wiley, 1951.

[4] J. Riordan, 同第一章参考文献[4].

第三章 递推关系

§1. 几个初等递推公式

公式

$$\binom{n}{r}=\binom{n-1}{r}+\binom{n-1}{r-1} \tag{1.1}$$

是递推关系的简单例子．从(1.1)以及适当的初始值，可以算出对所有非负整数 n，r 的二项式系数．其计算程序如杨辉三角所图示．其它许多种这类关系都叫递推关系，我们不必一定要对它下一个正式的定义．但大体上可以说，递推关系表示带整数参数的量的一类特殊关系，在这种关系下，可以从给出的初始值出发并依据前面已算出的值一步一步求出这个量．递推关系是从很多计数问题中自然产生的，关于它的理论有丰富的文献．本章后面所列的 Riordan 的著作[5]对此作了透彻的阐述．这里仅就几个特别使我们感兴趣的简单例子来讨论递推关系．

先看一个初等几何问题．我们要求确定平面上 n 条在一般位置上的直线能把这个平面划分成多少部分．记所分成的部分数为 P_n，我们定义

$$P_0=1. \tag{1.2}$$

不难验证，对每个正整数 n，有

$$P_n=P_{n-1}+n. \tag{1.3}$$

初始值(1.2)和递推关系(1.3)确定了 P_n 对所有非负整数 n 的值．事实上，从(1.2)，(1.3)可得

$$P_n=\frac{n(n+1)}{2}+1. \tag{1.4}$$

再看一个例子．令 T 表示整数 0 和 1 所组成的 2-集的所有 n 样品的集合．现在要来确定 T 中不含两个相继的 0 的样品的个数

记所求个数为 $f(n)$，我们定义

$$f(0)=1. \tag{1.5}$$

显然还有

$$f(1)=2. \tag{1.6}$$

现设 $n\geqslant 2$，则在所要求的 $f(n)$ 个样品中，第 1 个分量等于 1 的共有 $f(n-1)$ 个，第 1 个分量等于 0 的共有 $f(n-2)$ 个．于是

$$f(n)=f(n-1)+f(n-2). \tag{1.7}$$

初始条件 (1.5)，(1.6) 以及递推关系(1.7)确定了 $f(n)$ 对所有非负整数 n 的值． 数 $f(n)$ 叫作 Fibonacci 数．这些数有许多值得注意的算术性质和组合性质．

Euler 曾从递推关系的观点研究过更列个数 D_n．我们定义

$$D_0=1. \tag{1.8}$$

显然还有

$$D_1=0. \tag{1.9}$$

设有 n 个元素 $(n\geqslant 2)$ 1, 2…, n 的一个更列

$$(a_1, a_2, \cdots, a_n). \tag{1.10}$$

在式 (1.10) 中，第 1 个位置可取除 1 之外的任一其它 $n-1$ 个数．假定已取 $a_1=k(k\neq 1)$，则更列(1.10)可根据其第 k 个位置是否为 1 而分成两类．如果第 k 个位置上是 1，这种更列数为 $n-2$ 个元素的排列数，其中每个元素都不在它的自然位置上，因此共有 D_{n-2} 个．另一方面，如果第 k 个位置上不是 1，则这种更列就是元素 $1, 2, \cdots, k-1, k+1, \cdots, n$ 在第 2 到第 n 这 $n-1$ 个位置上的一个排列，其中 1 不在第 k 个位置上，其它元素都不在它自身所标记的位置上．这种排列相当于记为 $2, 3, \cdots, n$ 的这 $n-1$个元素的一个排列，其中每个元素都不在它的自然位置上．所以这一类更列共有 D_{n-1} 个．于是可得

$$D_n=(n-1)(D_{n-1}+D_{n-2}). \tag{1.11}$$

从 (1.11) 并利用归纳法可直接推出公式

$$D_n=n!\left(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+(-1)^n\frac{1}{n!}\right). \tag{1.12}$$

§2. 一个计数问题

设有记为 $1, 2, \cdots, n$ 的 n 个元素．令 U_n 为这 n 个元素的满足以下条件的排列个数： 元素 i 不在第 i 或第 $i+1$ 个位置上 $(1 \leqslant i \leqslant n-1)$，元素 n 不在第 n 或第 1 个位置上． 换句话说，U_n 是与下列两个排列

$$(1, 2, 3, \cdots, n), \qquad (n, 1, 2, \cdots, n-1) \tag{2.1}$$

处处不一致的排列的个数．分别用 C, J, I 记三种 n 阶 (0, 1)-方阵． 其中 C 在 $(1, 2), (2, 3), \cdots, (n, 1)$ 这 n 个位置上为 1，在其余位置为 0，J 在每个位置上都是 1． I 是 n 阶单位方阵．不难得出

$$U_n = \mathrm{per}(J - I - C). \tag{2.2}$$

但从第二章中积和式的公式还不能由 (2,2) 式直接求出 U_n.

数 U_n 有时被叫作"入座数"． 这个名词出自 Lucas 提出的下列"入座问题"： n 对夫妇围圆桌入座，要求男女相间，而且妇女都不坐在她丈夫身旁，问共有多少种入座法？ 可以让妇女先入座，这样有 $2 \cdot n!$ 种方式； 然后丈夫再入座，这时每个丈夫不能坐在他的妻子两边的位置上．另外，丈夫们的入座方法总数与妇女的坐法无关．如果用 M_n 来记"入座问题"所要求的入座方法总数，显然

$$M_n = 2 \cdot n! U_n. \tag{2.3}$$

因此我们只需集中讨论入座数 U_n.

定理 2.1. 入座数 U_n 由下式给出：

$$\begin{aligned} U_n = n! &- \frac{2n}{2n-1}\binom{2n-1}{1}(n-1)! \\ &+ \frac{2n}{2n-2}\binom{2n-2}{2}(n-2)! - \cdots \\ &+ (-1)^n \frac{2n}{n}\binom{n}{n} 0! \qquad (n > 1). \end{aligned} \tag{2.4}$$

公式(2.4)首先由 Touchard 得到，我们用 Kaplansky 的精巧的递推论证来证明它．先证两个引理．

引理 2.2. 设有 n 个元素排成一行. 现从中取出 k 个, 并要求这 k 个元素中没有两个在行中是相邻的. 设共有 $f(n, k)$ 种取法,则

$$f(n, k) = \binom{n-k+1}{k}. \tag{2.5}$$

证. 我们有初始条件

$$f(n, 1) = \binom{n}{1} = n, \tag{2.6}$$

以及当 $n > 1$ 时,有

$$f(n, n) = \binom{1}{n} = 0. \tag{2.7}$$

现设 $1 < k < n$. 我们可以把取法分成两类. 在一类取法中取出了第 1 个元素,因而一定不会取出第 2 个元素. 所以这类取法共有

$$f(n-2, k-1) \tag{2.8}$$

种. 在另一类取法中没有取出第 1 个元素,所以共有

$$f(n-1, k) \tag{2.9}$$

种取法. 于是我们得到递推公式

$$f(n, k) = f(n-1, k) + f(n-2, k-1). \tag{2.10}$$

现在可用归纳法来证明 (2.5). 根据归纳假设,我们有

$$f(n-1, k) = \binom{n-k}{k}, \ f(n-2, k-1) = \binom{n-k}{k-1}. \tag{2.11}$$

从(2.10)和(2.11)即得

$$f(n, k) = \binom{n-k}{k} + \binom{n-k}{k-1}. \tag{2.12}$$

这正等价于(2.5)式.

引理 2.3. 设有 n 个元素排成圆圈, 现从中取出 k 个, 并要求这 k 个元素中没有两个在圆圈中是相邻的. 设共有 $g(n, k)$ 种取法,则

$$g(n, k) = \frac{n}{n-k}\binom{n-k}{k} \qquad (n > k). \tag{2.13}$$

证．和前面一样，我们也把取法分成两类．在一类取法中取出了第1个元素，因而一定不会取出第2个或第n个元素．所以这类取法共有

$$f(n-3, k-1) \tag{2.14}$$

种．没有取出第1个元素的取法共有

$$f(n-1, k) \tag{2.15}$$

种．于是

$$g(n, k) = f(n-1, k) + f(n-3, k-1). \tag{2.16}$$

从(2.5)和(2.16)易得(2.13)．

我们再回到记为$1, 2, \cdots, n$的n个元素的排列问题上来．如果在一个排列中i在第i个位置上$(i = 1, 2, \cdots, n)$，则称此排列具有性质P_i.类似地，使i在第$i+1$个位置上$(i = 1, 2, \cdots, n-1)$的排列称作具有性质P'_i，使n在第1个位置上的排列称作具有性质P'_n．现将这$2n$个性质列成一行

$$P_1, P'_1, P_2, P'_2, \cdots, P_n, P'_n. \tag{2.17}$$

我们在这$2n$个性质中取出k个．如果这k个性质是相容的，则具有这k个性质的排列的个数等于$(n-k)!$，否则等于0．用v_k来记$2n$个性质(2.17)中取出k个相容性质的取法个数，则由筛式可得

$$\begin{aligned} U_m = v_0 n! - v_1(n-1)! + v_2(n-2)! \\ - \cdots + (-1)^n v_n 0!. \end{aligned} \tag{2.18}$$

再来计算v_k．注意到如果把$2n$个性质(2.17)排成圆圈，则只有处在相邻位置上的性质才是不相容的．从而由引理2.3可得

$$v_k = \frac{2n}{2n-k}\binom{2n-k}{k}. \tag{2.19}$$

定理2.1得证．

§3. 拉丁长方

设 S 是 n-集, A 是在 S 上的 $r \times s$ 长方阵列

$$A = [a_{ij}] \qquad (i = 1, 2, \cdots, r; j = 1, 2, \cdots, s). \tag{3.1}$$

如果 A 的每一行都是 S 的 n 个元素的 s-排列，同时 A 的每一列又都是 S 的 n 个元素的 r-排列，则称 A 为 S 上的一个**拉丁长方**. 当然这时必须要求 $r \leqslant n$, $s \leqslant n$. 如果 S 中的元素记为 $1, 2, \cdots, n$, 并假定 $s = n$, 则拉丁长方的每一行都是 $1, 2, \cdots, n$ 的一个排列，并且在同一列上元素不重复出现. 如果一个这类拉丁长方的第 1 行写成自然顺序 $1, 2, \cdots, n$, 则称这个拉丁长方为**规范化的**. 现分别用 $L(r, n)$ 和 $K(r, n)$ 记 $r \times n$ 拉丁长方和规范化的 $r \times n$ 拉丁长方的个数. 显然有

$$L(r, n) = n!K(r, n). \tag{3.2}$$

规范化的 $2 \times n$ 拉丁长方就是更列，于是

$$K(2, n) = D_n. \tag{3.3}$$

另外不难得知，入座数 U_n 等于前二行为

$$\begin{bmatrix} 1 & 2 & 3 \cdots & n \\ n & 1 & 2 \cdots n-1 \end{bmatrix} \tag{3.4}$$

的 $3 \times n$ 拉丁长方的个数. Riordan 得到 $K(3, n)$ 的一个有意义的公式

$$K(3, n) = \sum_{k=0}^{m} \binom{n}{k} D_{n-k} D_k U_{n-2k}, \tag{3.5}$$

其中 $m = \left[\frac{n}{2}\right]$, $U_0 = 1$. 但关于不止三行的拉丁长方的计数问题几乎没有触动，在这方面，应该提到 Erdős 和 Kaplansky 所得到的一个重要渐近公式：如果 $r < (\log n)^{\frac{3}{2}}$, 则有

$$L(r, n) = n!^r e^{-\binom{r}{2}}. \tag{3.6}$$

他们推测(3.6)式当 $r < n^{\frac{1}{3}}$ 时仍然成立，后来这由 Yamamoto 所证实.

如果 $r = s = n$, 则 $r \times s$ 拉丁长方称为 n **阶拉丁方**. 它可以

作为很一般的代数系统的乘法表．我们指出，有限群的乘法表确定了一个拉丁方，不过这样得到的拉丁方有很特殊的性质．

如果记

$$L(n, n) = n!(n-1)!l_n, \tag{3.7}$$

则 l_n 等于第 1 行和第 1 列都是自然顺序的 n 阶拉丁方的个数．当然，可以设想计算 l_n 不会是轻而易举的．事实上也是如此．下表是目前已知的全部 l_n 的值．

n	1	2	3	4	5	6	7
l_n	1	1	1	4	56	9408	16,942,080

参 考 文 献

Riordan 在[5]中对递推关系作了透彻的讨论，并有很多附加文献．Fibonnaci 数在 Dickson 的[1]，第十七章上有讨论．

关于数 U_n 的经典论文有 Touchard[7] 和 Kaplansky[3]．在 Riordan [4] 中有 $K(3, n)$ 公式的证明． $L(r, n)$ 的渐近公式可参看 Erdös 和 Kaplansky [2] 以及 Yamamoto[8]． l_7 的值取自 Sade[6]．

[1] L. E. Dickson，同第一章参考文献[1]．

[2] P. Erdös and I. Kaplansky, The asymptotic number of Latin rectangles, *Amer. Jour. Math.*, **68** (1946), 230—236.

[3] I. Kaplansky, Solution of the "Problème des ménages", *Bull. Amer. Math. Soc.*, **49**(1943), 784—785.

[4] J. Riordan, Three-line Latin rectangles-II, *Amer. Math. Monthly*, **53**(1946), 18—20.

[5] ———，同第一章参考文献[4]．

[6] A. Sade, Énumération des Carrés Latins. Application au 7ᵉ Ordre. Conjecture pour les Ordres Supérieurs, Marseille, 1948.

[7] J. Touchard, Sur un problème de permutations, *C. R. Acad. Sci. Paris*, **198** (1934), 631--633.

[8] K. Yamamoto, On the asymptotic number of Latin rectangles, *Japanese Jour. Math.*, **21**(1951), 113—119.

第四章 Ramsey 定理

§1. 基本定理

本节叙述并证明一个重要的组合定理，它来源于数学基础的研究．这个定理叫 Ramsey 定理，是英国逻辑学家 F. P. Ramsey 最早得到的．数学上的鸽笼原理说：如果把一个含有很多元素的集合划分成不多几个子集，那么至少在一个子集中含有相当数量的元素．Ramsey 定理可以看作是这个简单原理的深刻推广．Ramsey 定理的证明广泛使用递推技巧．这个定理应用很广，下一节讨论其中一部分应用．

设 S 是 n-集，$P_r(S)$ 是 S 的所有 r-子集的集．令

$$P_r(S) = A_1 \cup A_2 \cup \cdots \cup A_t \tag{1.1}$$

是 $P_r(S)$ 的一个任意的有序划分，这里 $A_1, \cdots, A_t$ 是 t 个分量．再令 $q_1, q_2, \cdots, q_t$ 是满足

$$1 \leqslant r \leqslant q_1, q_2, \cdots, q_t \tag{1.2}$$

的整数．如果有一个 S 的 q_i-子集，它的所有 r-子集都含在 A_i 中，则称这个 q_i-子集为 S 的 (q_i, A_i)-子集．Ramsey 定理的断言如下．

定理 1.1. 设给定了满足 (1.2) 的一组整数 $q_1, q_2, \cdots, q_t$ 和 r，则存在正整数 N，使得当 $n \geqslant N$ 时，对 n-集 S 的所有 r-子集的集 $P_r(S)$ 的任一有序划分 (1.1)，必有某个 $i (i = 1, 2, \cdots, t)$，使 S 包含一个 (q_i, A_i)-子集．

证．记具有上述性质的正整数 N 的最小者为 $N(q_1, q_2, \cdots, q_t, r)$．我们先分析一下 Ramsey 定理的种种特殊情形，以便对定理本身理解较深．首先，当 $r = 1$ 时，定理就是鸽笼原理．因为这时 $P_r(S)$ 就是 S，S 的一个 (q_i, A_i)-子集就是 A_i 的一个 q_i-子集．由此可得

$$N(q_1, q_2, \cdots, q_t, 1) = q_1 + q_2 + \cdots + q_t - t + 1. \tag{1.3}$$

其次，当 $q_1 = q_2 = \cdots = q_t = q \geqslant r \geqslant 1$ 时，定理 1.1 断言：设 S 是 n-集，如把 S 的所有 r-子集任意划分成 t 部分，则当 n 充分大时，一定存在 S 的一个 q-子集，它的所有 r-子集都含在这 t 部分的某一部分中．事实上，不难由此导出 Ramsey 定理的一般形式．为此可取 $q = \max(q_1, q_2, \cdots, q_t)$.

当 $t = 1$ 时，Ramsey 定理是显而易见的．这时可取 $N(q_1, r) = q_1$．假设定理当 $t = 2$ 时成立，则可知定理当 $t = 3$ 时也成立．因为这时可把 $P_r(S)$ 的划分写成

$$P_r(S) = A_1 \cup (A_2 \cup A_3). \tag{1.4}$$

再令

$$q_2' = N(q_2, q_3, r), \tag{1.5}$$

则当 $n \geqslant N(q_1, q_2', r)$ 时，n-集 S 必定含有某一个 (q_1, A_1)-子集或某一个 $(q_2', A_2 \cup A_3)$-子集．如果发生后一情况，S 的这一个 $(q_2', A_2 \cup A_3)$-子集必定含有某一个 (q_2, A_2)-子集或 (q_3, A_3)-子集．于是定理当 $t = 3$ 时也成立．由此不难归纳证明定理对所有 t 成立．所以我们只要集中力量来证明，当 $t = 2$ 时定理 1.1 成立．

由 (1.3) 式可知

$$N(q_1, q_2, 1) = q_1 + q_2 - 1. \tag{1.6}$$

另外，不难证明

$$N(q_1, r, r) = q_1, \tag{1.7}$$

$$N(r, q_2, r) = q_2. \tag{1.8}$$

例如，现在来证(1.7)式．这时令 $q_2 = r$，$n \geqslant q_1$．如果 A_2 非空，则 n-集 S 显然含有 (r, A_2)-子集．如果 A_2 是空集，则 $A_1 = P_r(S)$．从而 S 的任一 q_1-子集都是 S 的 (q_1, A_1)-子集．(1.7)证毕．同样可证 (1.8).

现在我们用归纳法来完成对 $t = 2$ 情形的证明．根据公式 (1.6)，(1.7) 和 (1.8)，可不妨假定所给的整数 q_1，q_2 和 r 满足严格不等式 $1 < r < q_1$，q_2，我们把整数 $N(q_1 - 1, q_2, r)$ 和 $N(q_1, q_2 - 1, r)$的存在，以及当整数 q_1'，q_2' 满足 $1 \leqslant r - 1 \leqslant q_1'$，

q_2'时，整数$N(q_1', q_2', r-1)$的存在作为归纳假设．根据这些假设，并利用公式(1.6)，(1.7)和(1.8)，即可证明整数$N(q_1, q_2, r)$的存在．在作出这个证明之前，可以先说明一下，以上的归纳论证是合理的．因为由此可知下列整数存在：

$$\begin{array}{llll} N(2,2,2), & N(2,3,2), & N(2,4,2), & \cdots \\ N(3,2,2), & N(3,3,2), & N(3,4,2), & \cdots \\ N(4,2,2), & N(4,3,2), & N(4,4,2), & \cdots \\ \vdots & \vdots & \vdots & \end{array} \tag{1.9}$$

从而又顺次可知所有$N(q_1, q_2, 3)$的存在，等等．

现在来完成上述归纳论证．根据归纳假设，我们已知$p_1 = N(q_1-1, q_2, r)$，$p_2 = N(q_1, q_2-1, r)$和$N(p_1, p_2, r-1)$都存在．现证$N(q_1, q_2, r)$存在．事实上，我们可以证明以下的递推不等式

$$N(q_1, q_2, r) \leqslant N(p_1, p_2, r-1) + 1. \tag{1.10}$$

设

$$n \geqslant N(p_1, p_2, r-1) + 1, \tag{1.11}$$

并设a是n-集S的一个确定的元素，T是S去掉元素a后的$(n-1)$-集．对$P_r(S)$的一个划分$P_r(S) = A_1 \cup A_2$，按下法可以确定$P_{r-1}(T)$的一个划分

$$P_{r-1}(T) = B_1 \cup B_2. \tag{1.12}$$

具体作法如下：对T的任一$(r-1)$-子集R，如果$R \cup a$在A_1中，则令$R \in B_1$；如果$R \cup a$在A_2中，则令$R \in B_2$．如此给出$P_{r-1}(T)$的划分(1.12)．

集合T至少有$N(p_1, p_2, r-1)$个元素．所以T一定含有一(p_1, B_1)-子集或含有一(p_2, B_2)-子集．假设T含有(p_1, B_1)-子集，即T含有一个p_1-子集U，U的所有$(r-1)$-子集都属于B_1．但$p_1 = N(q_1-1, q_2, r)$．所以U作为S的子集，一定含有一个其所有r-子集都在A_1中的(q_1-1)-子集或含有一个其所有r-子集都在A_2中的q_2-子集．若后一情况发生，则U的这个q_2-子集完全满足我们的要求，从而定理证毕．若前一情况发生，即U含有

一个 (q_1-1)-子集 V，V 的所有 r-子集都在 A_1 中．这时令 $W=V\cup a$，W 是 S 的 q_1-子集．对 W 的一个 r-子集，如果它不含 a，则它就是 V 的 r-子集，因而属于 A_1；如果它含有 a，则它是 a 和 V 的一个 $(r-1)$-子集的并，因为 V 是 U 的子集，所以 V 的所有 $(r-1)$-子集都属于 B_1，从而 W 的这个 r-子集是 a 和属于 B_1 的一个 $(r-1)$-子集的并．按照划分(1.12)的定义，W 的这个 r-子集一定在 A_1 中．于是 W 既是 S 的 q_1-子集，且其所有 r-子集又都在 A_1 中．

T 含有 (p_2, B_2)-子集的情形可完全仿此处理．至此完成了对 Ramsey 定理的证明．

整数 $N(q_1, q_2, r)$ 具有深刻的组合意义．遗憾的是我们不知道有关这些整数的任何递推公式，而递推不等式(1.10)在大多数场合又是不够精确的．因此计算 $N(q_1, q_2, r)$ 非常困难．当然我们已知道一批不足道的值(1.6)，(1.7)和(1.8)．除此之外，所有已知的 $N(q_1, q_2, r)$ 的值都列在下面关于 $N(q_1, q_2, 2)$ 的对称表中[1)]：

	3	4	5
3	6	9	14
4	9	18	
5	14		

(1.13)

对 $t>2$ 的情况所知更少是毫不足怪的．这方面目前所得到的主要结果是

$$N(3, 3, 3, 2)=17. \tag{1.14}$$

§2. 若干应用

考察三维空间中在一般位置上的 n 个点．将这 n 个点两两用线段连起来，并假设将每条线段染成红色或蓝色．这 n 个点的所

1) 还知道 $N(3, 6, 2)=N(4, 4, 2)=18$，$N(3, 7, 2)=23$．——译者注

有 2-集，也就是所有线段，可以划分成两部份 A_1 和 A_2，A_1 是所有红线段，A_2 是所有蓝线段. 设 q_1，q_2 是 $\geqslant 2$ 的整数. Ramsey 定理断言：当 $n \geqslant N(q_1, q_2, 2)$ 时，必有 q_1 个点，它们彼此都用红线段相连；或者有 q_2 个点，它们彼此都用蓝线段相连. 而且 $N(q_1, q_2, 2)$ 是具有这种性质的最小整数.

下面是 Ramsey 定理的一个有关凸多边形的应用.

定理 2.1. 设 m 是大于或等于 3 的整数，则存在正整数 N，使得当 $n \geqslant N$ 时，在平面上任何 3 点都不共线的 n 个点中，必有 m 个点是凸 m 边形的顶点.

引理 2.2. 设平面上有任何 3 点都不共线的 5 个点，则其中必有 4 点是凸四边形的顶点.

证. 两两连接这 5 点可得 10 根直线段，这个组态的周界一定是凸多边形. 如果它是凸五边形或凸四边形，引理已经得证. 假设它是三角形，则 5 点中余下 2 点必定在这个三角形的内部. 用一直线将这 2 个内点连起来，三角形必有 2 个顶点位于此直线的同侧. 于是这 2 个顶点和这 2 个内点是一个凸四边形的顶点.

引理 2.3. 设平面上有任何 3 点都不共线的 m 个点. 并且这 m 个点中的任意 4 点都是凸四边形的顶点，则此 m 个点是凸 m 边形的顶点.

证. 两两连接这 m 个点可得 $m(m-1)/2$ 根直线段. 设它们的周界是凸 q 边形. 并依次记此凸 q 边形的顶点为 $V_1, V_2, \cdots, V_q$. 如果原先的 m 个点中有一个在此凸 q 边形的内部，则它必在 $q-2$ 个三角形 $V_1V_2V_3$, $V_1V_3V_4$, $\cdots$, $V_1V_{q-1}V_q$ 中某一个的内部. 但这与假设矛盾. 所以 $q=m$，即这 m 个点是凸 m 边形的顶点.

根据这两个引理，定理 2.1 成为 Ramsey 定理的简单推论. 为了证明这一点，设 $m \geqslant 4$，并令 $n \geqslant N(5, m, 4)$，再把这 n 个点的 4-子集按其所构成的四边形是凹还是凸来作划分. Ramsey 定理断言，在这 n 点中，或者有 5 点. 其任意 4 点构成凹四边形；或者有 m 点，其任意 4 点构成凸四边形. 但引理 2.2 说明前面的情

形不会发生．而由引理2.3即得定理 2.1．

记定理 2.1 中的N的最小者为 N_m，则以上论证指出，

$$N_m \leqslant N(5, m, 4). \tag{2.1}$$

现在已经得到，$N_3 = 3 = 2 + 1$，$N_4 = 5 = 2^2 + 1$ 以及$N_5 = 9 = 2^3 + 1$．这使人们推测一般情形下有

$$N_m = 2^{m-2} + 1. \tag{2.2}$$

但这还是一个没有解决的问题．

最后讲一个有关(0,1)-矩阵的应用．n 阶方阵 A 的某个 m 阶子方阵称为主子方阵，如果这个 m 阶子方阵是由 A 划去 $n-m$ 行和同样的 $n-m$ 列后所得．

定理 2.4. 对任意给定的正整数 m，只要 n 充分大，每个 n 阶(0,1)-方阵必含有形如下列四类之一的 m 阶主子方阵：

$$\begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix}, \begin{pmatrix} * & & 0 \\ & \ddots & \\ 1 & & * \end{pmatrix}, \begin{pmatrix} * & & 1 \\ & \ddots & \\ 0 & & * \end{pmatrix}, \begin{pmatrix} * & & 1 \\ & \ddots & \\ 1 & & * \end{pmatrix}. \tag{2.3}$$

在(2.3)式中，主对角线上的元素可以为 0，也可以为 1．但主对角线以上和主对角线以下的元素一定全为 0 或全为 1，具体四种类型按 (2.3) 所示．

证．现将$A = [a_{ij}]$ 的 n 个行向量的集取作 Ramsey 定理中的 n-集 S．记A的第 i 行为 α_i．对 A 中两个行向量 α_i 和 α_j，当 $i<j$ 时，附以向量 (a_{ji}, a_{ij})．这种二维向量只可能有四种情形：(0, 0)，(1, 0)，(0, 1) 或 (1,1)．根据所附向量的四种情形，可将 A 的每两个行向量区分为四种情形．因而我们有 n-集 S 的所有 2-子集的一个划分

$$P_2(S) = A_1 \cup A_2 \cup A_3 \cup A_4. \tag{2.4}$$

根据 Ramsey 定理，如果

$$n \geqslant N(m, m, m, m, 2). \tag{2.5}$$

则必有 S 的某个 m-子集，它的所有 2-子集全部含在 $P_2(S)$ 的同一分量 $A_i (i = 1, 2, 3, 4)$ 之中．这正说明 A 含有(2.3)所列的一种 m 阶主子方阵．

参 考 文 献

最初形式的 Ramsey 定理发表在 [8]. 我们的证明和有关凸多边形的结果取自 Erdös 和 Szekeres 的[4]. 值 $N(q_1, q_2, 2)$ 和 $N(3, 3, 3, 2)$ 的计算可见 Greenwood 和 Gleason 的[6].

[1] P. Erdös and R. Rado, A combinatorial theorem, *Jour. London Math. Soc.*, **25** (1950), 249—255.

[2] ——————, Combinatorial theorems on classifications of subsets of a given set, *Proc. London Math. Soc. 3rd seriers*, **2** (1952), 417—439.

[3] ——————, A partition calculus in set theory, *Bull. Amer. Math. Soc.*, **62** (1956), 427—489.

[4] P. Erdös and G. Szekeres, A combinatorial problem in geometry, *Compositio Mathematica*, **2** (1935), 463—470.

[5] A. W., Goodman, On sets of acquaintances and strangers at any party, *Amer. Math. Monthly*, **66** (1959), 778—783.

[6] R. E. Greenwood and A. M. Gleason, Combinatorial relations and chromatic graphs, *Canad. Jour. Math.*, **7** (1955), 1—7.

[7] R. Rado, Direct decomposition of partitions, *Jour. London Math. Soc.*, **29** (1954), 71—83.

[8] F. P. Ramsey, On a problem of formal logic., *Proc. London Math. Soc.*, 2nd stries, **30** (1930), 264—286.

[9] T. Skolem, Ein Kombinatorischer Satz mit Anwendung auf ein logisches Entscheidungsproblem, *Fundamenta Mathematicae*, **20** (1933), 254—261.

第五章 相异代表组

§1. 基本定理

设 S 是任意集，$P(S)$ 是 S 的所有子集的集. 又设

$$D = (a_1, a_2, \cdots, a_m) \tag{1.1}$$

是 S 的一个 m-样品，

$$M(S) = (S_1, S_2, \cdots, S_m) \tag{1.2}$$

是 $P(S)$ 的一个 m-样品. 假定 D 的 m 个元素互异，并且

$$a_i \in S_i \qquad (i = 1, 2, \cdots, m), \tag{1.3}$$

则元素 a_i 代表了集合 S_i，我们说子集 $S_1, S_2, \cdots, S_m$ 有一个相异代表组 (*system of distinct representatives*，简记为 *SDR*)，并称 D 是 $M(S)$ 的一个 *SDR*. *SDR* 的定义本身要求当 $i \neq j$ 时 $a_i \neq a_j$，但 S_i 和 S_j 不必一定是 S 的不同子集.

我们对 *SDR* 概念作一个简单的说明. 设 S 是 1,2,3,4,5 组成的 5-集；$S_1 = \{2, 5\}$, $S_2 = \{2, 5\}$, $S_3 = \{1, 2, 3, 4\}$, $S_4 = \{1, 2, 5\}$. 则 $D = (2, 5, 3, 1)$ 是 (S_1, S_2, S_3, S_4) 的一个 *SDR*. 如果把上述 S_4 改成 $S_4' = \{2, 5\}$，则 (S_1, S_2, S_3, S_4') 不再有 *SDR*. 因为这时 $S_1 \cup S_2 \cup S_4'$ 是 2-集，而至少要 3 个元素才能代表 S_1, S_2 和 S_4'.

下述 P. Hall 的基本定理给出了存在 *SDR* 的充分必要条件.

定理 1.1. 子集 $S_1, S_2, \cdots, S_m$ 有 *SDR* 的充分必要条件是：对任一整数 k，$1 \leqslant k \leqslant m$，以及对 $\{1, 2, \cdots, m\}$ 的任一 k-子集 $\{i_1, i_2, \cdots, i_k\}$，并集 $S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_k}$ 至少含有 k 个元素.

基本定理的必要性是显然的. 在下述的定理 1.2 中，我们将不仅证明充分性，同时还给出 *SDR* 个数的一个正的下界. 本章其余部分将讨论基本定理的进一步发展和应用.

定理 1.2. 设子集 $S_1, S_2, \cdots, S_m$ 满足有 SDR 的必要条件，并设每个集 S_i 至少有 t 个元素，则当 $t \leqslant m$ 时，$M(S)=(S_1, S_2, \cdots, S_m)$ 至少有 $t!$ 个 SDR；当 $t>m$ 时，$M(S)$ 至少有 $t!/(t-m)!$ 个 SDR.

证 对m进行归纳证明. 当 $m=1$ 时，定理显然成立. 作为归纳假设，设定理对 $P(S)$ 的所有 m'-样品成立，这里 $m'<m$. 现证定理对m-样品 $M(S)=(S_1, S_2, \cdots, S_m)$ 成立. 分两种情形讨论.

第一种情形：假定对任一整数 $k(1 \leqslant k \leqslant m-1)$，以及对 $\{1, 2, \cdots, m\}$的任一 k-组合 $\{i_1, i_2, \cdots, i_k\}$，并集 $S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_k}$ 至少含有 $k+1$ 个元素. 这时，我们先在 S_1 中取定一个元素 a_1. 再定义 $S_j'=S_j \backslash\{a_1\}(j=2, 3, \cdots, m)$. 不难验证，$(m-1)$-样品

$$M'(S)=(S_2', S_3', \cdots, S_m') \tag{1.4}$$

仍满足有 SDR 的必要条件. 如果 $t \leqslant m$，则 $t-1 \leqslant m-1$. 根据归纳假设，$M'(S)$ 至少有 $(t-1)!$ 个 SDR；如果 $t>m$，则 $t-1>m-1$. 同样根据归纳假设，$M'(S)$ 至少有 $(t-1)!/(t-m)!$ 个 SDR. 但 $M'(S)$ 的一个 SDR 连同代表 S_1 的 a_1 是 $M(S)=(S_1, S_2, \cdots, S_m)$ 的一个 SDR，在 S_1 中每取一个元素 a_1，以上结论都成立. 由于 S_1 至少有 t 个元素，故得 $M(S)$的 SDR 个数的所需估计.

第二种情形：假定有一个整数 $k(1 \leqslant k \leqslant m-1)$，以及 $\{1, 2, \cdots, m\}$ 的一个 k-组合 $\{i_1, i_2, \cdots, i_k\}$，并集 $S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_k}$ 是 k-集. 这时，我们可不妨假定$S_1 \cup S_2 \cup \cdots \cup S_k$是 k-集. 有这个 k-集本身就表明 $t \leqslant k$. 根据归纳假设，k-样品 $(S_1, S_2, \cdots, S_k)$ 至少有 $t!$ 个 SDR. 设 $D^*=(a_1, a_2, \cdots, a_k)$ 是其中一个 SDR. 对 $j=k+1, k+2, \cdots$，在 S_j 中去掉 D^* 中的元素后所得的集记为 S_j^*. 我们说，$(m-k)$-样品

$$M^*(S)=(S_{k+1}^*, S_{k+2}^*, \cdots, S_m^*) \tag{1.5}$$

满足有 SDR 的必要条件. 因为，假如并集 $S_{k+1}^* \cup S_{k+2}^* \cup \cdots \cup S_{k+k^*}^*$

的元素个数小于 k^*，则并集

$$S_1 \cup S_2 \cup \cdots \cup S_k \cup S_{k+1} \cup S_{k+2} \cup \cdots \cup S_{k+k^*} \qquad (1.6)$$

的元素个数小于 $k + k^*$，而这与定理的假设矛盾．因此，根据归纳假设，$M^*(S)$ 至少有一个 SDR．所以 $M(S)$ 至少有 $t!$ 个 SDR．定理 1.2 证毕．

§2. 划分的公共代表组

设

$$T = A_1 \cup A_2 \cup \cdots \cup A_m \qquad (2.1)$$

和

$$T = B_1 \cup B_2 \cup \cdots \cup B_m \qquad (2.2)$$

是集合 T 的两个划分，其中 A_i，B_j 都不是空集 $(i, j = 1, 2, \cdots, m)$．如果有 T 的一个 m-子集 E，E 满足 $A_i \cap E \neq \emptyset$，$B_j \cap E \neq \emptyset (i, j = 1, 2, \cdots, m)$，则这 $2m$ 个非空交集都是 1-集，我们称 E 为划分 (2.1) 和 (2.2) 的**公共代表组** (*system of common representatives*，简记为 SCR)．易知划分(2.1)和(2.2)有 SCR 当且仅当存在划分 (2.1) 的 m 个分量的重新标号，使在新标号下

$$A_i \cap B_i \neq \emptyset \qquad (i = 1, 2, \cdots, m). \qquad (2.3)$$

我们用上节关于 SDR 的基本定理来得出下述 SCR 存在的充分必要条件．

定理 2.1. 划分 (2.1) 和 (2.2) 有 SCR 的充分必要条件是：对任一整数 k，$1 \leqslant k \leqslant m$，以及对 $\{1, 2, \cdots, m\}$ 的任一 k-子集 $\{i_1, i_2, \cdots, i_k\}$，并集 $A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_k}$ 至多包含 m 个子集 B_1，B_2，$\cdots$，B_m 中的 k 个．

证　定理的必要性仍是显然的．现证充分性．设 S 是元素为 A_1，A_2，$\cdots$，A_m 的 m-集．又设 S_i 是 S 的子集，S_i 的元素是 A_1，A_2，$\cdots$，A_m 中使 $A_j \cap B_i \neq \emptyset$ 的所有 A_j，则 $M(S) = (S_1, S_2, \cdots, S_m)$ 是 $P(S)$ 的一个 m-样品．我们说，子集 S_1，S_2，$\cdots$，S_m 满足有 SDR 的必要条件．假如不满足，可不妨设 $S_1 \cup S_2 \cup \cdots \cup S_{k+1}$ 只含有 k 个元素 A_{i_1}，A_{i_2}，$\cdots$，A_{i_k}．根据 S_i 的定义，这说明并集

$A_{i_1}\cup A_{i_2}\cup\cdots\cup A_{i_k}$包含 $k+1$ 个集合 $B_1, B_2, \cdots, B_{k+1}$. 从而与定理的假设矛盾. 根据定理 1.1,子集 $S_1, S_2, \cdots, S_m$ 一定有一个 SDR. 我们可以对划分 (2.1) 的 m 个分量重新标号,使这个 SDR 在新标号下是 $D=(A_1, A_2, \cdots, A_m)$. 这说明 (2.3) 成立,从而定理 2.1 得证.

定理 2.2. 设 $T=A_1\cup A_2\cup\cdots\cup A_m$ 和 $T=B_1\cup B_2\cup\cdots\cup B_m$ 是 T 的两个划分. 如果其中每个子集 A_i 和 B_j 都是 T 的 r-子集,则这两个划分有 SCR.

证 这是定理 2.1 的特殊情形.

由定理 2.2 可知,设 A 是在整数集上的一个 $r\times m$ 阵列

$$A=\begin{bmatrix} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & 2m \\ \vdots & \vdots & & \vdots \\ (r-1)m+1 & (r-1)m+2 & \cdots & rm \end{bmatrix}. \tag{2.4}$$

如果 B 也是一个元素为 $1, 2, \cdots, rm$ 的 $r\times m$ 阵列, 不过 rm 个数 $1, 2, \cdots, rm$ 任意分布在 B 的 rm 个位置上. 则一定可对 B 作列的排列, 使得 A 和经列排列后的 B 在标号相同的每一列上至少有一个公共元素.

下一个例子要求懂一点群的陪集的初等性质,它也是定理 2.2 的直接推论.

定理 2.3. 设 G 是有限群, H 是 G 的一个子群. 又设

$$G=Hx_1\cup Hx_2\cup\cdots\cup Hx_m$$

是 G 对 H 的右陪集分解, $G=y_1H\cup y_2H\cup\cdots\cup y_mH$ 是 G 对 H 的左陪集分解,则 G 必有 m 个元 $z_1, z_2, \cdots, z_m$, 使

$$G=Hz_1\cup Hz_2\cup\cdots\cup Hz_m=z_1H\cup z_2H\cup\cdots\cup z_mH. \tag{2.5}$$

§3. 拉丁长方

在本节,我们把 SDR 理论用于讨论拉丁长方. 设给定一个在 n 个整数 $1, 2, \cdots, n$ 上的 $r\times s$ 拉丁长方, 如果在这个拉丁长方上可以添加 $n-r$ 行和 $n-s$ 列而得到一个 n 阶拉丁方, 并使原

先的 $r \times s$ 拉丁长方位于 n 阶拉丁方的左上角，则我们称这个 $r \times s$ 拉丁长方可以扩充为一个 n 阶拉丁方.

定理 3.1. 在 n 个整数 $1, 2, \cdots, n$ 上的任一 $r \times n$ 拉丁长方,必可扩充为一个 n 阶拉丁方.

证 设 S 是元素为 $1, 2, \cdots, n$ 的 n-集. 又设 S_i 是 S 中所有不在拉丁长方的第 i 列上的元素的集合,则每个 S_i 都是 S 的 $(n-r)$-子集. $M(S) = (S_1, S_2, \cdots, S_n)$ 是 S 的子集的一个 n-样品. 我们证明 $M(S)$ 满足有 SDR 的必要条件. S 中的一个元素 i 在 $r \times n$ 拉丁长方的每一行上出现一次,而且它又都位于不同列上. 所以 i 含在 n 个集合 $S_1, S_2, \cdots, S_n$ 的 $(n-r)$ 个之中. 假如 $M(S)$ 不满足定理 1.1 的条件,不妨设 $S_1 \cup S_2 \cup \cdots \cup S_k$ 只有 $k' < k$ 个元素. 那末这 k' 个元素一方面在 $S_1, S_2, \cdots, S_k$ 中应该总共出现 $(n-r)k$ 次;另一方面，这 k' 个元素在 $S_1, S_2, \cdots, S_k$ 中又至多出现 $(n-r)k'$ 次,这是矛盾. 所以 $M(S)$ 一定有 SDR. 如记 $M(S)$ 的一个 SDR 为 $D = (i_1, i_2, \cdots, i_n)$,则可将 D 作为第 $r+1$ 行添加到原先给定的 $r \times n$ 拉丁长方上去,得 $(r+1) \times n$ 拉丁长方. 这个过程可以一直进行下去，直到扩充成 n 阶拉丁方为止.

定理 3.2. 至少存在

$$n!(n-1)!\cdots(n-r+1)! \tag{3.1}$$

个 $r \times n$ 拉丁长方,从而至少存在

$$n!(n-1)!\cdots 1! \tag{3.2}$$

个 n 阶拉丁方.

证 易见有 $n!$ 个 $1 \times n$ 拉丁长方. 根据定理 3.1 和定理 1.2,每个 $1 \times n$ 拉丁长方至少可以扩充为 $(n-1)!$ 个 $2 \times n$ 拉丁长方,因而至少存在 $n!(n-1)!$ 个 $2 \times n$ 拉丁长方. 如此继续讨论,即证定理.

设 l_n 是第 1 行第 1 列都是自然顺序的 n 阶拉丁方的个数，则定理 3.2 断言

$$l_n \geqslant (n-2)!(n-3)!\cdots 1!. \tag{3.3}$$

下表列出了当 $n=3,4,5,6,7$ 时，$b_n=(n-2)!(n-3)!\cdots 1!$ 和 l_n 的值.

n	3	4	5	6	7
l_n	1	4	56	9408	16,942,080
b_n	1	2	12	288	34,560

§4. (0, 1)-矩阵

设 A 是 $m\times n$ 型的(0,1)-矩阵.这种矩阵之所以在组合数学中很起作用,其主要原因之一如下所述.设 S 是元素为 $a_1,a_2,\cdots,a_n$ 的 n-集，$M(S)=(S_1,S_2,\cdots,S_m)$ 是 S 的子集的 m-样品. 如果 $a_j\in S_i$，则令 $a_{ij}=1$；如果 $a_j\notin S_i$，则令 $a_{ij}=0$. 于是可得 $m\times n$ 型的(0,1)-矩阵

$$A=[a_{ij}]\qquad (i=1,2,\cdots,m;\ j=1,2,\cdots,n).\qquad (4.1)$$

这个矩阵称为 n-集 S 关于它的 m 个子集 $S_1,S_2,\cdots,S_m$ 的关联矩阵. A 的第 i 行上的 1 指出了属于 S_i 的元素，A 的第 j 列上的 1 指出了包含 a_j 的子集. 因此 A 已将 S 的子集 $S_1,S_2,\cdots,S_m$ 刻画无遗.反过来，如果给定一个 $m\times n$ 型的(0,1)-矩阵 A,并有一任意 n-集 S，则一定有 S 的子集 $S_1,S_2,\cdots,S_m$，使 A 是关于这些子集的关联矩阵.

由此可知,(0,1)-矩阵 A 表征了 S 的子集 $S_1,S_2,\cdots,S_m$. 当然,如果我们不用 0，1 而用其它两个量，如 $+1$，-1 或 x，y 来构作关联矩阵，也能完全表征这些子集. 但这样做通常并不会更方便. 事实上,取(0,1)-矩阵作为关联矩阵特别合适,因为 0 和 1 的加法和乘法性质极简单. 下列定理可以说明这点.

定理 4.1. 设 $S_1,S_2,\cdots,S_m$ 是 n-集 S 的子集，$m\leqslant n$. A 是关于这些子集的关联矩阵，则 $M(S)=(S_1,S_2,\cdots,S_m)$ 的 SDR 个数等于 $\operatorname{per}(A)$.

证　这是所用术语的定义的直接推论. 并注意到 $\operatorname{per}(A)$ 的定义和 SDR 的存在都要求 $m\leqslant n$.

如果一个 $m\times n$ 型的 (0, 1)-矩阵 P 满足 $PP^T=I$，这里 I 是

$m\times m$ 的单位方阵，则称 P 为置换矩阵. 由定义本身可知 $m\leqslant n$，而且 $m\times n$ 置换矩阵的每一行，每一列都只有一个 1.

设 $m\times n$ 型的 (0, 1)-矩阵 A 是关于 $S_1, S_2, \cdots, S_m$ 的关联矩阵. 如对 S 的 n 个元素以及对 S 的 m 个子集重新标号，则关联矩阵 A 变为另一个关联矩阵 A'，它形如

$$A'=PAQ. \tag{4.2}$$

这里 P 是由子集的重新标号所决定的 n 阶置换方阵，Q 是由元素的重新标号所决定的 n 阶置换方阵. 许多关于(0,1)-矩阵 A 的研究所涉及的都是像 per(A) 这种在行与列的排列下不变的函数，其原因现在清楚了. 这些函数所以在组合数学中有意义，是因为它们与 S 的元素及子集的标号方法无关.

§5. 项秩

矩阵的一行或一列都称为矩阵的一条. 一个矩阵的迹是这个矩阵的主对角线上的元素之和. 设 A 是 $m\times n$ 型的(0, 1)-矩阵. A 中两两不在同一条上的 1 的最大个数定义为 A 的项秩(*term rank*). 根据这个定义，可知 A 的项秩等于 A 在任意的行和列的排列下的迹的最大值. 另外，A 的项秩也等于 A 的具有非零积和式的子方阵的最大阶数. 项秩的概念可以作为 n-集 S 的子集 $S_1, S_2, \cdots, S_m$ 的 SDR 概念的合适推广. 因为如记这些子集的关联矩阵为 A，则这些子集有 SDR 当且仅当 A 的项秩等于 m.

定理 5.1. 设 A 是 $m\times n$ 型的 (0, 1)-矩阵，则 A 的能包含 A 中所有的 1 的条的最小个数等于 A 的项秩.

证 记能包含 A 中所有的 1 的条的最小个数为 ρ'，又记 A 的项秩为 ρ. 我们要证 $\rho=\rho'$. 首先，没有一条能包含体现项秩的一组 ρ 个 1 中的两个，所以 $\rho'\geqslant\rho$. 现在我们用 SDR 理论来证 $\rho\geqslant\rho'$. 设能用 A 的 e 行和 f 列包含 A 的所有的 1，这里 $e+f=\rho'$. 由于 ρ 和 ρ' 在 A 的行和列的置换下都不变，因此不妨假定这 e 行和 f 列是 A 的前 e 行和前 f 列. 这时将 A 记成分块形式

$$\begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}, \tag{5.1}$$

其中 A_1 是 $e \times f$ 矩阵．现证 A_2 的项秩为 e．为此我们可将 A_2 看作整数 $f+1, f+2, \cdots, n$ 的 $(n-f)$-集的子集 $S_1, S_2, \cdots, S_e$ 的关联矩阵．这些子集一定满足存在 SDR 的必要条件．因为要是不满足的话，我们可以在原来的 e 行 f 列中将这 e 行代之以个数较少的列而仍能包含 A 中所有的 1．但后者是由少于 $e+f$ 条组成，这与 ρ' 的定义矛盾．同样地，可以将 A_3 的转置 A_3^T 看作 f 个子集的关联矩阵，并证明 A_3 的项秩是 f．于是 $\rho \geqslant e+f=\rho'$，从而定理 5.1 得证．

定理 5.1 有如下直接推广．设 A 是元素在域 F 中的 $m \times n$ 矩阵，则 A 的能包含 A 中所有非零元素的条的个数的最小值等于 A 中两两不在同一条上的一组非零元素的个数的最大值．

定理 5.2. 设 A 是元素为非负实数的 $m \times n$ 矩阵 $(m \leqslant n)$，A 的每行的行和都等于 m'，每列的列和都等于 n'，则 A 一定可以表为

$$A = c_1P_1 + c_2P_2 + \cdots + c_tP_t, \tag{5.2}$$

其中 P_i 是置换矩阵，c_i 是非负实数 $(i = 1, 2, \cdots, t)$．

证　如果 A 不是方阵，我们可把 A 换成

$$A' = \begin{bmatrix} A \\ \frac{m'}{n} J \end{bmatrix}, \tag{5.3}$$

这里 J 是元素全是 1 的 $(n-m) \times n$ 矩阵．现在 A' 是元素为非负实数的 n 阶方阵，而且 A' 的行和与列和都是 m'．我们说，只要 A' 不是零方阵，A' 一定有 n 个两两不在同一条上的正元素．因为要是没有这样的 n 个元素的话，由定理 5.1 的推广可知，A' 可以用 e 行和 f 列覆盖所有非零元素，这里 $e+f<n$．从而导致 $m'n \leqslant m'(e+f) < m'n$ 的矛盾．现作一个 n 阶置换方阵 P_1'．P_1' 的 n 个 1 与 A' 的上述 n 个正元素在同样的位置上，再令 c_1 是 A' 中那 n 个正元素的最小者，则 $A'-c_1P_1'$ 是元素为非负实数的 n 阶方阵，其

行和与列和都等于非负实数 $m'-c_1$，而且 $A'-c_1P'_1$ 至少比 A' 多一个0．我们再用同法讨论 $A'-c_1P'_1$．这样继续下去，直到 $A'-c_1P'_1-c_2P'_2-\cdots-c_tP'_t$ 成为零方阵．这就证明了 A 的分解式 (5.2)．

定理 5.2 有一些有意义的应用．

定理 5.3. 设 A 是 n 阶 (0,1)-方阵．A 的行和与列和都等于正整数 k，则 A 可表为

$$A=P_1+P_2+\cdots+P_k, \tag{5.4}$$

这里 P_i 都是置换方阵．

证 在定理 5.2 的证明中，每个 $c_i=1$，而且进行了 $t=k$ 步后就得出零方阵．故得定理 5.3．

定理 5.3 给下述问题以肯定回答．设有 n 个男孩和 n 个女孩参加一次舞会．每个男孩事先恰好认识 k 个女孩，每个女孩也恰好认识 k 个男孩，大家都不想和事先不认识的人对舞，问能否在一次对舞中，使每个男孩的舞伴都是事先已认识的女孩？记 $A=[a_{ij}]$ 是这样一个 n 阶 (0, 1)-方阵：如男孩 j 和女孩 i 事先认识，则 $a_{ij}=1$，否则 $a_{ij}=0$．显然，A 满足定理 5.3 的条件，并且 (5.4) 式中的置换方阵 P_1 可用来决定哪些男孩和女孩结为舞伴．

如果一个元素为非负实数的 n 阶方阵 A 的行和与列和都等于1，则称 A 是**双随机的**．由于它在转移概率的理论中的重要性，双随机矩阵已被广泛地研究．从定理 5.2 可以推出下列有关双随机矩阵的结果．

定理 5.4. 设 A 是 n 阶双随机方阵，则 A 可表成

$$A=c_1P_1+c_2P_2+\cdots+c_tP_t, \tag{5.5}$$

这里 P_i 是置换方阵，c_i 是满足

$$c_1+c_2+\cdots+c_t=1 \tag{5.6}$$

的正实数．

证 设 A 是双随机方阵．由于 A 的元素都是非负实数，所以 per(A) 不超过 A 的行和的乘积．又由于 A 的行和都等于1，所以

$$\text{per}(A)\leqslant 1. \tag{5.7}$$

(5.7)式中等号成立当且仅当双随机方阵 A 是置换方阵. 另外, 由定理 5.4 易知 $\mathrm{per}(A) > 0$. 但对 n 阶双随机方阵 A, 如何确定 $\mathrm{per}(A)$ 的最小值是一个没有解决的难题[1). van der Waerden 猜想下列不等式成立:

$$\mathrm{per}(A) \geqslant \frac{n!}{n^n}. \tag{5.8}$$

其中等号成立当且仅当 $A = n^{-1}J$. 这个猜想还可以推广为: 对双随机方阵 A 与 B, 有

$$\mathrm{per}(AB) \leqslant \mathrm{per}(A), \ \mathrm{per}(B). \tag{5.9}$$

如取 $B = m^{-1}J$, 则 (5.9) 式等价于 (5.8) 式.

参 考 文 献

基本定理 1.1 是 P. Hall[8] 给出的. 定理 1.2 由 M. Hall[6] 给出, 这里对定理 1.2 的证明取自 Halmos 和 Vaughan[9]以及 Mann 和 Ryser[15]. 在拉丁长方中的应用根据 M. Hall[5, 6]. 在矩阵中的许多应用根据 König[14]. 在 Marcus 和 Newman 的[17, 18]中对 van der Waerden 猜想进行了广泛的探讨.

[1] C. Berge, Théorie des Graphes et Ses Applications, Paris, Dunod, 1958. (中译本: 图的理论及其应用, 上海科学技术出版社, 1963.)

[2] C. J. Everett and G. Whaples, Representations of sequences of sets, *Amer. Jour. Math*, **71** (1949), 287—293.

[3] L. R. Ford, Jr. and D. R. Fulkerson, Network flows and systems of representatives, *Canad. Jour. Math*, **10** (1958), 78—85.

[4] ——————, Flows in Networks, Princeton University Press, 1962.

[5] M. Hall, Jr., An existence theorem for Latin squares, *Bull. Amer. Math. Soc.*, **51** (1945), 387—388.

[6] ——————, Distinct representaives of subsets, *Bull. Amer. Math. Soc.*, **54** (1948), 922—926.

[7] ——————, An algorithm for distinct representatives, *Amer. Math. Monthly*, **63** (1956), 716—717.

[8] P. Hall, On representatives of subsets, *Jour. London Math. Soc.*, **10** (1935), 26—30.

[9] P. R. Halmos and H. E. Vaughan, The marriage problem, *Amer Jour. Math.*, **72** (1950), 214—215.

[10] P. J. Higgins, Disjoint transversals of subsets, *Canad, Jour. Math.*, **11** (1959), 280—285.

[11] A. J. Hoffman, Some recent applications of the theory of linear inequa-

1) 这个猜想近年已得证实. 请参看 125 页的注. ——译者注

lities to extremal combinatorial analysis, *Proc. of Symposia in Applied Math.*, **10** (1960), 113—128.
[12] A. J. Hoffman and H. W. Kuhn, Systems of distinct representatives and linear programming, *Amer. Math. Monthly*, **63** (1956), 455—460.
[13] ——————, On systems of disrinct representatives, *Annals of Math. Studies*, no. **38** (1956), 199— 206.
[14] D. König, Theorie der Endlichen und Unendlichen Grahen, New York, Chelsea, 1950.
[15] H. B. Mann and H. J. Ryser, Systems of distinct representatives, Amer. *Math. Monthly*, **60** (1953), 397—401.
[16] M. Marcus and H. Minc, On the relation between the determinant and the permanent, *Illinois Jour. Math.*, **5** (1961), 376—381.
[17] M. Marcus and M. Newman, On the minimum of the permanent of a doubly stochastic matrix, *Duke Math. Jour.*, **26** (1959), 61—72.
[18] ——————, Inequalities for the permanent function, *Ann. Math.*, **75** (1962), 47—62.
[19] N. S. Mendelsohn and A. L. Dulmage, Some generalizations of the problem of distinct representatives, *Canad. Jour. Math.*, **10** (1958), 230—241.
[20] O. Ore, Graphs and matching theorems, *Duke Math. Jour.*, **22** (1955), 625—639.
[21] ——————, Theory of Graphs, *Amer. Math. Soc. Colloq. Publs.*, **38**, 1962.
[22] R. Rado, Factorization of even graphs, *Quarterly Jour. Math.*, **20** (1949), 95—104.
[23] H. J. Ryser, A combinatorial theorem with an application to Latin rectangles, *Proc. Amer. Math. Soc.*, **2** (1951), 550—552.

第六章　(0,1)-矩阵

§1. 类 $\mathfrak{A}(R, S)$

设 A 是 $m \times n$ 型的 $(0, 1)$-矩阵. 记 A 的第 i 行元素之和为 r_i, 第 j 列元素之和为 s_j. 我们称向量

$$R = (r_1, r_2, \cdots, r_m) \tag{1.1}$$

为 A 的**行和向量**,称向量

$$S = (s_1, s_2, \cdots, s_n) \tag{1.2}$$

为 A 的**列和向量**. 如果 $r_1 \geqslant r_2 \geqslant \cdots \geqslant r_m$, 则称 R 是**单调的**.同样,当 $s_1 \geqslant s_2 \geqslant \cdots \geqslant s_n$ 时,称 S 是单调的. 令 τ 是 A 中所有 1 的个数,显然

$$\tau = \sum_{i=1}^{m} r_i = \sum_{j=1}^{n} s_j. \tag{1.3}$$

行和向量等于 R, 列和向量等于 S 的所有 $m \times n$ 型的$(0,1)$-矩阵组成一个类,记为

$$\mathfrak{A} = \mathfrak{A}(R, S). \tag{1.4}$$

在这一章中, 我们将研究类 $\mathfrak{A}$ 的结构. 所论定理虽然仅与 $(0, 1)$-矩阵有关, 但每个结论都能用纯组合用语重述为集合与元素的组合结论,因为每个 $m \times n$ 型的$(0, 1)$-矩阵都可以作为一个 n-集 T 的子集 $T_1, T_2, \cdots, T_m$ 的关联矩阵.

现给定两个向量 $R = (r_1, r_2, \cdots, r_m)$, $S = (s_1, s_2, \cdots, s_n)$, R 与 S 的分量都是非负整数. $\mathfrak{A} = \mathfrak{A}(R, S)$ 是行和向量及列和向量分别等于 R 及 S 的所有 $m \times n$ 型的 $(0, 1)$-矩阵的类. 我们来研究类 $\mathfrak{A}$ 非空的条件. 先引进一些记号. 令 n 维行向量

$$\delta_i = (1, 1, \cdots, 1, 0, 0, \cdots 0) \qquad (i = 1, 2, \cdots, m), \tag{1.5}$$

其中 δ_i 的前 r_i 个分量是 1,其余分量是 0. 形如

$$A = \begin{bmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \delta_m \end{bmatrix} \tag{1.6}$$

的矩阵称为极大的，并称 $\bar{A}$ 为具有行和向量 R 的极大矩阵. $\bar{A}$ 的列和向量 $\bar{S}=(\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_n)$ 显然是单调的. 而且

$$\sum_{i=1}^{m} r_i = \sum_{j=1}^{n} \bar{s}_j, \tag{1.7}$$

类 $\mathfrak{A}(R, \bar{S})$ 只含 $\bar{A}$ 一个矩阵. 设 $S=(s_1, s_2, \cdots, s_n)$ 和 $S^*=(s_1^*, s_2^*, \cdots, s_n^*)$ 是分量为非负整数的两个向量. 如果对足标适当重新标号后，以下关系成立

$$s_1 \geqslant s_2 \geqslant \cdots \geqslant s_n, \quad s_1^* \geqslant s_2^* \geqslant \cdots \geqslant s_n^*, \tag{1.8}$$

$$s_1+s_2+\cdots+s_i \leqslant s_1^*+s_2^*+\cdots+s_i^* \quad (i=1,2,\cdots,n-1), \tag{1.9}$$

$$s_1+s_2+\cdots+s_n = s_1^*+s_2^*+\cdots+s_n^*, \tag{1.10}$$

则称 S 为 S^* 所优超，记为

$$S \prec S^*. \tag{1.11}$$

定理 1.1. 设 $R=(r_1, r_2, \cdots, r_m)$ 和 $S=(s_1, s_2, \cdots, s_n)$ 是分量为非负整数的两个向量. 又设 $\bar{A}$ 是行和向量等于 R，列和向量等于 $\bar{S}$ 的极大矩阵，则类 $\mathfrak{A}(R,S)$ 非空的充分必要条件是

$$S \prec \bar{S}. \tag{1.12}$$

证　如果 $\mathfrak{A}$ 含有一个矩阵 A，则 A 可由 $\bar{A}$ 在各行上移动其 1 的位置而得出. 于是，对单调的 S，我们有

$$s_1+s_2+\cdots+s_i \leqslant \bar{s}_1+\bar{s}_2+\cdots+\bar{s}_i \quad (i=1,2,\cdots,n-1), \tag{1.13}$$

$$s_1+s_2+\cdots+s_n = \bar{s}_1+\bar{s}_2+\cdots+\bar{s}_n. \tag{1.14}$$

即 $S \prec \bar{S}$.

如果已知 $S \prec \bar{S}$，经重新标号后，可设 R 和 S 都是单调的. 我们来构作一个行和向量等于 R 且列和向量等于 S 的矩阵 $\tilde{A}$. 我们用把 $\bar{A}$ 的每一行上的 1 逐次向右移动的方法来构作 $\tilde{A}$. 先叙述具

体作法．然后再证明它是实际可行的．首先在 $\bar{A}$ 中依次把行和最大的 s_n 个行的最后一个1移到第 n 列，遇到有些行的行和相等时，则优先移动它们中最下面那一行的最后一个 1．于是 $\bar{A}$ 变成形如

$$[\bar{A}_{n-1},\ A_1] \tag{1.15}$$

的矩阵．其中 A_1 是 $m\times 1$ 矩阵，其列和是 s_n．$\bar{A}_{n-1}$ 是 $m\times(n-1)$ 极大矩阵．然后把 A_1 放置不动，用同法变动 $\bar{A}_{n-1}$．如此进行了 $n-f$ 步后，$\bar{A}$ 已经变成形如

$$[\bar{A}_f,\ A_{n-f}] \tag{1.16}$$

的矩阵．其中 A_{n-f} 是 $m\times(n-f)$ 矩阵，它有单调的列和向量 $(s_{f+1}, s_{f+2}, \cdots, s_n)$．$\bar{A}_f$ 是 $m\times f$ 极大矩阵．现在来进行第 $n-f+1$ 步，并证明它是实际可行的．假如当我们按前面所说的步骤变动 $\bar{A}_f$ 时，不能使第 f 列的列和变成 s_f．记 $\bar{A}_f$ 的列和向量为 $(e_1, e_2, \cdots, e_f)$．这时必定 $e_1<s_f$ 或 $e_f>s_f$．如果 $e_1<s_f$，则

$$\begin{aligned} s_1+s_2+\cdots+s_f&=e_1+e_2+\cdots+e_f\leqslant fe_1<fs_f\\ &\leqslant s_1+s_2+\cdots+s_f, \end{aligned} \tag{1.17}$$

这是一个矛盾．另一方面，如果 $e_f>s_f$，则 $e_f>s_{f+1}, s_{f+2},\cdots,s_n$，所以 A_{n-f} 的前 e_f 行所成的子矩阵中，每一列至少有一个 0．矩阵 $\bar{A}_f$ 是行和向量单调的极大矩阵．因此根据我们逐步构造的方式，可知 A_{n-f} 的后 $m-e_{f-1}$ 行全是 0，于是

$$e_1+e_2+\cdots+e_{f-1}=\bar{s}_1+\bar{s}_2+\cdots+\bar{s}_{f-1}. \tag{1.18}$$

上式结合(1.12)可得

$$\begin{aligned} s_1+s_2+\cdots+s_{f-1}+s_f&=e_1+e_2+\cdots+e_{f-1}+e_f\\ &\leqslant\bar{s}_1+\bar{s}_2+\cdots+\bar{s}_{f-1}+s_f\\ &=e_1+e_2+\cdots+e_{f-1}+s_f. \end{aligned} \tag{1.19}$$

从而得到 $s_f\geqslant e_f$，而这与 $e_f>s_f$ 矛盾．所以我们一定可以从构作第 n 列开始，而这个过程自动终止于第 1 列．注意到在我们所构作的 $\tilde{A}$ 中，它的前 i 列的行和向量 $R_i(i=1, 2, \cdots, n)$ 都是单调的．

矩阵

$$\tilde{A}=\begin{bmatrix}1&1&1&0\\1&1&0&1\\1&0&0&0\\0&1&0&0\end{bmatrix}\tag{1.20}$$

可作为在 $R=S=(3,3,3,1)$ 时上述构作方法的例.

本节我们确定了类 $\mathfrak{A}$ 非空的条件. 困难得多的问题是确定这个非空类中矩阵的个数, 它无疑将是 R 和 S 的一个极复杂的函数.

§2. 对拉丁长方的一个应用

设有在元素为 $1,2,\cdots,n$ 的 n-集上的 $r\times s$ 拉丁长方. 本节给出它可以扩充成 n 阶拉丁方的充分必要条件.

定理 2.1. 设 A 是 $m\times n$ 型的 $(0,1)$-矩阵, $m\leqslant n$. A 的行和向量 $R=(k,k,\cdots,k)$, k 是正整数. A 的列和向量 $S=(s_1,s_2,\cdots,s_n)$, 其中

$$0\leqslant k-s_i\leqslant n-m\qquad(i=1,2,\cdots,n),\tag{2.1}$$

则 A 一定可以表为 k 个置换矩阵 P_i 之和

$$A=P_1+P_2+\cdots+P_k.\tag{2.2}$$

证 如果 $m=n$, 上述定理就是第五章的定理 5.3. 因此现在可不妨假定 $m<n$. 我们说, 这时一定有一个 $(n-m)\times n$ 型的 $(0,1)$-矩阵 A', A' 的行和向量 $R'=(k,k,\cdots,k)$, A' 的列和向量 $S'=(k-s_1,k-s_2,\cdots,k-s_n)$. 因为如令 $\bar{S}'$ 是一个前 k 个分量为 $n-m$, 其余 $n-k$ 个分量为 0 的向量, 由 (2.1) 可知 $S'\prec\bar{S}'$, 从而由定理 1.1 可知 A' 一定存在. 现在 n 阶方阵

$$\begin{bmatrix}A\\A'\end{bmatrix}\tag{2.3}$$

的每个行和与每个列和都等于 k, 根据第五章定理 5.3, 它是 k 个置换方阵之和. 从而 A 也是 k 个置换矩阵之和.

定理 2.2. 设在元素为 $1,2,\cdots,n$ 的 n-集上有一 $r\times s$ 拉丁长方. 以 $N(i)$ 记数 i 在此拉丁长方中出现的次数, 则此拉丁长

方可以扩充为 n 阶拉丁方的充分必要条件是

$$N(i) \geqslant r + s - n \qquad (i = 1, 2, \cdots, n). \tag{2.4}$$

证 记 $1, 2, \cdots, n$ 所组成的 n-集为 T. 又记 T 中不在拉丁长方的第 i 行中出现的元素的集为 $T_i(i = 1, 2, \cdots, r)$, 则 T_i 都是 T 的 $(n - s)$-子集. 设 r 个集合 $T_1, T_2, \cdots, T_r$ 中有 $M(i)$ 个含 $i(i = 1, 2, \cdots, n)$. 如果拉丁长方可以扩充为 n 阶拉丁方, 则 $M(i) \leqslant n - s$. 但 $N(i) + M(i) = r$, 所以 $N(i) \geqslant r + s - n$.

反过来, 如果有 $N(i) \geqslant r + s - n$. 设 A 是关于 n-集 T 的子集 $T_1, T_2, \cdots, T_r$ 的关联矩阵, 则 $r \times n$ 矩阵 A 的行和向量 $R = (n - s, n - s, \cdots, n - s)$, A 的列和向量 $S = (M(1), M(2), \cdots, M(n))$. 由假定可知 $N(i) = r - M(i) \geqslant r + s - n$, 又从拉丁长方与 $N(i)$ 的定义可知 $N(i) = r - M(i) \leqslant s$, 所以

$$0 \leqslant n - s - M(i) \leqslant n - r \qquad (i = 1, 2, \cdots, n). \tag{2.5}$$

根据定理 2.1, A 可以表为 $n - s$ 个置换矩阵之和:

$$A = P_1 + P_2 + \cdots + P_{n-s}. \tag{2.6}$$

但式(2.6)中的每个置换矩阵都确定了 $1, 2, \cdots, n$ 的一个 r-排列, 把这 $n - s$ 个 r-排列作为 $n - s$ 列添加到 $r \times s$ 拉丁长方上可得 $r \times n$ 拉丁长方. 再根据第五章定理 3.1, 这个 $r \times n$ 拉丁长方又可以扩充为 n 阶拉丁方. 或者我们也可以不用第五章的定理 3.1, 将这个 $r \times n$ 拉丁方转置后再扩充为 n 阶拉丁方, 这时关于 $N(i)$ 的条件显然成立.

从上述定理可以提出下列更一般的问题: 设有一个元素为 $1, 2, \cdots, n$ 和 x 的 $n \times n$ 阵列. 现在要问, 在什么条件下我们可以把这些 x 分别适当改成 $1, 2, \cdots, n$ 中的数而得到 n 阶拉丁方? 定理 2.2 解决了一种非常特殊的情况, 对一般问题的处理迄今都不成功[1].

---

1) 这就是不完全(即带有空位)的 n 阶拉丁方在什么条件下可以扩充为一个 n 阶拉丁方的问题. 近来 Smetaniuk 证明了, 任一在 $n-1$ 个位置上已确定的带空位的 n 阶拉丁方, 一定可以扩充为 n 阶拉丁方. 从而解决了已有 20 多年的一个猜想[3]. 见 *Ars Combinatoria*, 11(1981), 155—172.——译者注

§ 3. 对换

设 $\mathfrak{A}=\mathfrak{A}(R, S)$ 是行和向量为 $R=(r_1, r_2, \cdots, r_m)$，列和向量为 $S=(s_1, s_2, \cdots, s_n)$ 的所有 $m\times n$ 型的(0，1)-矩阵的类，$A\in\mathfrak{A}$. 考察 A 的如下 2×2 子方阵

$$A_1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad A_2=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}. \tag{3.1}$$

把 A 中某个形如 A_1(或 A_2) 的子方阵变为 A_2(或 A_1)，同时使 A 的其它元素不变的变换称为一个**对换**. 在一定的意义下，对换是那些作用在 A 上后使所得矩阵仍在类 $\mathfrak{A}$ 中的运算中最基本的一种. 对换在处理很多有关类 $\mathfrak{A}$ 的问题时很有用. 我们先建立下述对换定理.

定理 3.1. 设 A 和 A' 都属于 $\mathfrak{A}(R, S)$，则可用有限次对换把 A 变成 A'.

证 不妨设 R 与 S 都是单调的. 设 $\tilde{A}$ 如定理 1.1 所构作. 我们一定可以用有限次对换把 A 变成 $\tilde{A}$. 事实上，可用若干次对换把 A 的第 n 列变成 $\tilde{A}$ 的第 n 列. 这是因为 $\tilde{A}$ 的第 n 列上的 1 在 s_n 个行和最大的行上. A 经过这些对换后，第 n 列与 $\tilde{A}$ 的第 n 列相同，从而其前 $n-1$ 列所成 $m\times(n-1)$ 矩阵与 $\tilde{A}$ 的前 $n-1$ 列所成的 $m\times(n-1)$ 矩阵有相同的行和向量与列和向量. 根据 $\tilde{A}$ 的构造，又可用若干次对换把前者的第 $n-1$ 列变成 $\tilde{A}$ 的第 $n-1$ 列. 这样经过有限次对换后，我们可把 A 变成 $\tilde{A}$. 类似地可用有限次对换把 A' 变成 $\tilde{A}$. 当然反过来也可用有限次对换把 $\tilde{A}$ 变成 A'. 这样总能用有限次对换把 A 变成 A'. 我们说，把 A 变成 A' 所需对换的最少次数显然将是一个 A 与 A' 的极复杂的函数.

设矩阵 A 属于类 $\mathfrak{A}(R, S)$. 在很多场合中，我们都可以不妨假定 A 的行和向量 R 与列和向量 S 满足

$$r_1\geqslant r_2\geqslant\cdots\geqslant r_m>0, \tag{3.2}$$

$$s_1\geqslant s_2\geqslant\cdots\geqslant s_n>0. \tag{3.3}$$

这说明 A 既排除了全是零的行或列，又有单调的行和向量与列和

向量．满足(3.2)及(3.3)式的非空类 $\mathfrak{A}(R, S)$ 称为**规范的**．在今后的讨论中，我们都假定 $\mathfrak{A}$ 是规范的．

设 A 属于规范类 $\mathfrak{A}$． A 在 (e, f) 位置上的元数 a_{ef} 如果是 1，而且对 A 进行任何对换都不能把 a_{ef} 变成 0，则称 a_{ef} 是一个**不变量 1**．根据对换定理 3.1，这时 $\mathfrak{A}$ 中每个矩阵在 (e, f) 处的元素都是不变量 1．所以 $\mathfrak{A}$ 的所有矩阵或者全都没有不变量 1，或者都有不变量 1，我们可以说 $\mathfrak{A}$ 没有或有不变量 1．

定理 3.2. 规范类 $\mathfrak{A}$ 有不变量 1 的充分必要条件是，$\mathfrak{A}$ 中每个矩阵 A 都可以表为

$$A = \begin{bmatrix} J & * \\ * & 0 \end{bmatrix}. \tag{3.4}$$

这里 J 是元素全是 1 的 $e \times f$ 矩阵 $(0 < e \leqslant m;\ 0 < f \leqslant n)$．整数 e, f 不一定是唯一的，但它们都由行和向量 R 与列和向量 S 所确定，并与 A 在 $\mathfrak{A}$ 中的选取无关．

证 显然，形如式 (3.4) 的矩阵中，J 里的每个 1 都是不变量 1．反过来，如果 $\mathfrak{A}$ 有不变量 1，设 a_{ef} 是使 $e + f$ 最大的一个不变量 1．对 $\mathfrak{A}$ 中任一矩阵 A，记

$$A = \begin{bmatrix} W & X \\ Y & Z \end{bmatrix}, \tag{3.5}$$

其中 W 是 $e \times f$ 矩阵，则 W 必等于 J，而且 W 的全部元素都是不变量 1．因为要是 W 中有 0 的话，由于 $\mathfrak{A}$ 是规范的，至多经过两次对换就可以把 a_{ef} 变为 0．现在因为 $e + f$ 最大，我们可以在 $\mathfrak{A}$ 中取一个 A，使 A 表成式(3.5)时在 X 的第 1 列上有 0． 这时如果在 Z 的第 t 行中有 1，至多经过一次对换，可以假定这个 1 在 Z 的第一列．这样 Y 的第 t 行一定全是 1．因为要是在 Y 的第 t 行中有 0，则可用对换改变 W 中的不变量 1．事实上这时 Y 的第 t 行中的每个 1 都是不变量 1．但这与 $e + f$ 的最大性矛盾．所以 $Z = 0$ 且 A 形如式(3.4)．从而 $\mathfrak{A}$ 中每个矩阵都形如式 (3.4)．

§4. 最大项秩

设 $\tilde{\rho}$ 和 $\bar{\rho}$ 分别是规范类 $\mathfrak{A} = \mathfrak{A}(R, S)$ 中矩阵的最小项秩和

最大项秩．在这一节里我们来分析 $\bar{\rho}$．下述定理本身有其意义并导出 $\bar{\rho}$ 的一个精确公式．而且推导这些结果的方法对若干有关问题也是有用的．我们先叙述一个关于中间项秩的初等结果．

定理 4.1. 设 $\tilde{\rho}$ 和 $\bar{\rho}$ 分别是规范类 $\mathfrak{A}$ 中矩阵的最小项秩和最大项秩，则对区间

$$\tilde{\rho} \leqslant \rho \leqslant \bar{\rho} \tag{4.1}$$

中的任一整数 ρ，在 $\mathfrak{A}$ 中必有矩阵 A_ρ，其项秩等于 ρ.

证　对 $\mathfrak{A}$ 中矩阵进行一次对换，矩阵的项秩或者不变，或者增减 1．根据对换定理，我们可用有限次对换把 $\mathfrak{A}$ 中项秩等于 $\bar{\rho}$ 的矩阵 $A_{\bar{\rho}}$ 变成项秩等于 $\tilde{\rho}$ 的矩阵 $A_{\tilde{\rho}}$．故必有矩阵 A_ρ 的项秩等于 ρ.

定理 4.2. 规范类 $\mathfrak{A}$ 中有矩阵 $A_{\bar{\rho}}$，它在$(1,\bar{\rho})$，$(2,\bar{\rho}-1)$，$\cdots$，$(\bar{\rho},1)$这 $\bar{\rho}$ 个位置上都是 1.

证　设 $A_{\bar{\rho}}$ 是具有最大项秩 $\bar{\rho}$ 的一个矩阵，我们在 $A_{\bar{\rho}}$ 中取出 $\bar{\rho}$ 个两两不在同一条上的 1，称这 $\bar{\rho}$ 个 1 是本质的 1，其余的 1 称为非本质的．我们一定可以在 $\mathfrak{A}$ 中选取一个 $A_{\bar{\rho}}$，使得 $A_{\bar{\rho}}$ 的 $\bar{\rho}$ 个本质的 1 在前 $\bar{\rho}$ 行中．因为要是有一个本质的 1 在(i, j)位置处，而在第 i' 行上没有本质的 $1(i' \leqslant \rho < i)$．若在 (i', j) 处是 1，则我们可以改取这个 1 作为本质的 1，使原来在 (i, j) 处的 1 变成非本质的．若在 (i', j) 处是 0，由于 $\mathfrak{A}$ 是规范的，则经过一次对换后，一定可以在 (i', j) 处有本质的 1 并使项秩 $\bar{\rho}$ 不变．循此我们可以得到一个在前 $\bar{\rho}$ 行有 $\bar{\rho}$ 个本质的 1 的矩阵 $A_{\bar{\rho}}$．类似地讨论列，则在 $\mathfrak{A}$ 中有矩阵

$$A_{\bar{\rho}} = \begin{bmatrix} D & * \\ * & 0 \end{bmatrix}, \tag{4.2}$$

其中 D 是项秩为 $\bar{\rho}$ 的 $\bar{\rho}$ 阶方阵．0 是零矩阵，因为 $A_{\bar{\rho}}$ 的项秩不可能超过 $\bar{\rho}$.

我们称在 $(1, \bar{\rho})$，$(2, \bar{\rho}-1)$，$\cdots(\bar{\rho}, 1)$ 这 $\bar{\rho}$ 个位置的元素构成 D 的次对角线．现在来证明可以取得形如 (4.2) 的矩阵 $A_{\bar{\rho}}$，它的 $\bar{\rho}$ 个本质的 1 在 D 的次对角线上．假设在 D 的$(1,\bar{\rho})$，$(2,\bar{\rho}-$

$1), \cdots, (d, \bar{\rho} - d + 1)$ 位置上是本质的 1，而在 $(d + 1, \bar{\rho} - d)$ 处不是本质的 1，则在第 $d + 1$ 行和第 $\bar{\rho} - d$ 列上各有一个本质的 1. 这两个本质的 1 所在的 D 的 2 阶子方阵不外下列四种形式，而这两个本质的 1 总在主对角线上：

$$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\ \begin{bmatrix}1 & 0\\1 & 1\end{bmatrix},\ \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix},\ \begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}. \qquad (4.3)$$

至多对 $A_{\bar{\rho}}$ 作一次对换，可以使 D 的上述 2 阶子方阵的次对角线上的两个元素都是 1，并可把这两个 1 替换原在主对角线上的两个本质的 1 作为 $A_{\bar{\rho}}$ 的新的本质的 1. 这样就在 D 的 $(d + 1, \bar{\rho} - d)$ 处也有了本质的 1，于是证明了在 $\mathfrak{A}$ 中存在 $A_{\bar{\rho}}$，它的 $\bar{\rho}$ 个本质的 1 在 D 的次对角线上. 定理 4.2 证毕.

设 Q 是一个 $(0, 1)$-矩阵，我们用 $N_0(Q)$ 记 Q 中 0 的个数，用 $N_1(Q)$ 记 Q 中 1 的个数. 又设 A 是 $m \times n$ 型的 $(0,1)$-矩阵，我们总假定 $m, n > 0$. 不过当对矩阵作分块时，允许有退化的 $e \times f$ 子矩阵，即允许 e 或 f 等于 0. 对退化子矩阵 W，约定 $N_0(W) = N_1(W) = 0$. 下述定理是关于规范类中矩阵的最大项秩的主要结果.

定理 4.3. 规范类 $\mathfrak{A}$ 中每个矩阵 A 都可以分块为

$$A = \begin{bmatrix}W & X\\Y & Z\end{bmatrix}, \qquad (4.4)$$

这里 W 是 $e \times f$ 矩阵 $(0 \leqslant e \leqslant m; 0 \leqslant f \leqslant n)$，$Z$ 是 $(m - e) \times (n - f)$ 矩阵，而且

$$N_0(W) + N_1(Z) = \bar{\rho} - (e + f). \qquad (4.5)$$

整数 e 和 f 不一定是唯一的，但它们都由行和向量 R 与列和向量 S 所确定，而与 A 在 $\mathfrak{A}$ 中的选取无关. 特别地，定理 4.2 中的 $A_{\bar{\rho}}$ 满足

$$N_0(W) = 0, \qquad N_1(Z) = \bar{\rho} - (e + f). \qquad (4.6)$$

证　设 A 的行和向量 $R = (r_1, r_2, \cdots, r_m)$，列和向量 $S = (s_1, s_2, \cdots, s_n)$，则显见有

$$N_0(W) + N_1(Z) = ef + (r_{e+1} + r_{e+2} + \cdots + r_m) - (s_1 + s_2 + \cdots + s_f). \qquad (4.7)$$

所以 $N_0(W) + N_1(Z)$ 与 $\mathfrak{A}$ 中矩阵 A 的选取无关．因此我们只需证明定理对定理 4.2 中所指出的矩阵 $A_{\bar{p}}$ 成立．现对 $A_{\bar{p}}$ 的行数用归纳法．对只有 1 行的矩阵 $A_{\bar{p}}$，定理一定成立．如果定理对 $m-1$ 行的矩阵 $A_{\bar{p}}$ 成立，我们来证明定理对 m 行的 $A_{\bar{p}}$ 也成立．这时，如果 $\bar{p}=m$，则可取 $e=m$，$f=0$ 而使定理成立．同样地，如果 $\bar{p}=n$，则可取 $e=0$，$f=n$ 而使定理成立． 为此我们可假定 $\bar{p}<m,n$．注意在这种情形下，定理中的 e 和 f 必定作出 $A_{\bar{p}}$ 的一个非退化的分块，即有 $0<e<m$，$0<f<n$． 因为要是 $e=0$ 或 m，或者 $f=0$ 或 n 的话，将导致与 $\bar{p}<m,n$ 矛盾．

现设定理 4.2 中所指出的矩阵 $A_{\bar{p}}=[a_{ij}]$ 的项秩 $\bar{p}<m,n$，我们用下述方法使 $A_{\bar{p}}$ 的第一行规范化：如果 $a_{1i}=0$，$a_{1j}=1$ 而 $s_i>s_j$，则可用一次对换把 a_{1i} 换成 1，a_{1j} 换成 0． 而且如果这时 $i<\bar{p}$，则这个对换一定可以选得使 $A_{\bar{p}}$ 在 $(\bar{p}-i+1,\ i)$ 处的本质的 1 不动．同样，如果当 $i<j$ 时，有 $s_i=s_j$，$a_{1i}=1$，$a_{1j}=0$，则可以用一次对换把 a_{1i} 换成 0，a_{1j} 换成 1．如果这时 $j<\bar{p}$，而且这个对换不能选得使 $A_{\bar{p}}$ 在 $(\bar{p}-j+1,\ j)$处的本质的 1 不动，则 $A_{\bar{p}}$ 在 $(\bar{p}-i+1,\ j)$ 处必是 1，从而我们可以在进行上述对换后、再用一次涉及第 $\bar{p}-i+1$ 行和第 $\bar{p}-j+1$ 行的对换，使在 $(\bar{p}-j+1,\ j)$ 处重新换成 1． 当我们把上面所讲的所有可能的对换都进行过后，得到一个如下形状的矩阵

$$M=\begin{bmatrix}\delta_1 & \delta_2\\ A_{\bar{p}-1} & 0\end{bmatrix}. \tag{4.8}$$

在(4.8)式中，δ_1 是 $1\times n'$ 矩阵，δ_2 是元素都是 1 的 $1\times(n-n')$ 矩阵． 这时并不排除 $n=n'$ 的退化情况． $(m-1)\times n'$ 矩阵 $A_{\bar{p}-1}$ 在 $(1,\bar{p}-1)$，$(2,\bar{p}-2)$，$\cdots(\bar{p}-1,1)$ 这 $\bar{p}-1$ 个位置上有 1．右下角的 0 是 $(m-1)\times(n-n')$ 的零矩阵．

矩阵 $A_{\bar{p}-1}$ 产生一个规范类 $\mathfrak{A}'$，我们证明，$\bar{p}-1$ 是 $\mathfrak{A}'$ 中矩阵的最大项秩．要是 $\mathfrak{A}'$ 中有矩阵 A'，它在 $(1,\bar{p})$，$(2,\bar{p}-1)$，$\cdots$，$(\bar{p},1)$ 处有 $\bar{p}$ 个本质的 1． 我们把 (4.8) 式中的 $A_{\bar{p}-1}$ 换成 A'，记所得矩阵为 M'．矩阵 M' 属于类 $\mathfrak{A}$． 如果 M' 在 $(1,n)$ 处是 0，

则总可以用一次对换使 $(1, n)$ 处是 1，这样，M' 的项秩必大于 $\bar{\rho}$，这与 $\bar{\rho}$ 是 $\mathfrak{A}$ 的最大项秩矛盾. 所以，$\mathfrak{A}'$ 的最大项秩是 $\bar{\rho}-1$，而 $A_{\bar{\rho}-1}$ 达到这个最大项秩，并在 $(1, \bar{\rho}-1), (2, \bar{\rho}-2), \cdots, (\bar{\rho}-1, 1)$ 处有 $\bar{\rho}-1$ 个本质的 1. 根据归纳假设，$A_{\bar{\rho}-1}$ 可以表为

$$A_{\bar{\rho}-1}=\begin{bmatrix} W' & X' \\ Y' & Z' \end{bmatrix}, \tag{4.9}$$

其中 $e' \times f'$ 矩阵 W' 的元素都是 1，$N_1(Z')=\bar{\rho}-1-(e'+f')$. 我们还把上述 f' 尽可能地取得大，使得在 Z' 中的每个本质的 1 所在的那一列上方，X' 至少有一个 0. 我们知道 $\bar{\rho}-1<m-1$，但有可能 $\bar{\rho}-1=n'$. 后一情况导致 $A_{\bar{\rho}-1}$ 具有 $e'=0, f'=n'$ 的退化分块. 而对于其它情况，必有 $0<e'<m-1, 0<f'<n'$.

如果在 (4.8) 中 δ_1 含有这样一个 0，这个 0 位于 Y' 的某一列的上方，而 Y' 的这一列又有一个 $A_{\bar{\rho}-1}$ 的非本质的 1，则根据我们对 M 的第一行所作的规范化，必有 $n'=n$，而且在 δ_1 的 $f'+1, f'+2, \cdots, n$ 处都是 0. 当 $A_{\bar{\rho}-1}$ 有退化分块时，上述事实与 $\bar{\rho}-1=n'$ 矛盾；当 $A_{\bar{\rho}-1}$ 的分块非退化时，上述事实又与 $r_1 \geqslant r_2$ 矛盾. 因此，如果在 Y' 的某一列的上方 δ_1 有 0，则 Y' 的这一列上没有 $A_{\bar{\rho}-1}$ 的非本质的 1. 这意味着总可以把 $A_{\bar{\rho}-1}$ 的分块 (4.9) 调整得使 M 在 Y' 的上方的 δ_1 中不含 0. 如果 M 在 $(1, \bar{\rho})$ 处是 1，则已得所要求的分块；如果 M 在 $(1, \bar{\rho})$ 处是 0，则可用一次对换使 M 在 $(1, \bar{\rho})$ 处是 1. 这给出了我们想要的分块.

作为定理 4.3 的一个简单的推论，我们可以得到一个值得注意的公式，它用行和向量 $R=(r_1, r_2, \cdots, r_m)$ 与列和向量 $S=(s_1, s_2, \cdots, s_n)$ 的分量把规范类 $\mathfrak{A}(R, S)$ 的最大项秩 $\bar{\rho}$ 表示出来.

定理 4.4. 记

$$t_{ij}=ij+(r_{i+1}+r_{i+2}+\cdots+r_m)-(s_1+s_2+\cdots+s_j)$$
$$(i=0, 1, \cdots, m; j=0, 1, \cdots, n), \tag{4.10}$$

则

$$\bar{\rho}=\min_{i,j}\{t_{ij}+(i+j)\}$$
$$(i=0, 1, \cdots, m; j=0, 1, \cdots, n). \tag{4.11}$$

证　设矩阵

$$A_p = \begin{bmatrix} W & X \\ Y & Z \end{bmatrix} \tag{4.12}$$

具有最大项秩 $\bar{\rho}$，其中 W 是 $i \times j$ 矩阵，则可用 $\bar{\rho}$ 条覆盖住 A_p 的全部 1．因此

$$N_1(Z) + (i + j) \geqslant \bar{\rho}. \tag{4.13}$$

但 $N_0(W) \geqslant 0$，所以

$$t_{ij} + (i + j) \geqslant \bar{\rho}. \tag{4.14}$$

在(4.14)中，如取 i, j 为定理 4.3 中所说的 e, f，则等号成立．故定理 4.4 得证．

也可以得出计算 $\tilde{\rho}$ 的公式，但我们在这里不深究了．下述定理给出 $\tilde{\rho} < \bar{\rho}$ 的条件．

定理 4.5.　设规范类 $\mathfrak{A}$ 没有不变量 1，而且 $\bar{\rho} < m, n$，则 $\tilde{\rho} < \bar{\rho}$．

证　根据 $\bar{\rho} < m, n$ 的假设，定理 4.3 中的 e, f 满足 $0 < e < m$，$0 < f < n$．同时根据定理的假设，定理 4.3 中的 A_p 在(1,1)处不是不变量 1．但定理 4.3 断言 $N_0(W) + N_1(Z) = \bar{\rho} - (e+f)$．以上事实说明在 $\mathfrak{A}$ 中一定有一个矩阵，它在 Z 中 1 的个数小于 $\bar{\rho} - (e + f)$．因此这个矩阵一定可以用少于 $\bar{\rho}$ 条覆盖住全部 1．所以 $\tilde{\rho} < \bar{\rho}$．

注意在定理 4.5 中，关于没有不变量 1 的假设是必不可缺的．例如仅由极大矩阵 $\bar{A}$ 一个矩阵构成的类就有 $\tilde{\rho} = \bar{\rho}$．同样，$\bar{\rho} < m, n$ 的限制也是不可少的．例如，$n!$ 个 n 阶置换方阵构成的类就有 $\tilde{\rho} = \bar{\rho}$．用 $\tilde{\rho} = \bar{\rho}$ 把全部 $\mathfrak{A}(R, S)$ 作一个干净利落的分类乃是一个未解决而又有意义的问题[1]．

§ 5. 有关问题

前一节分析了规范类 $\mathfrak{A}$ 中矩阵 A 的项秩．我们还可以指出 A 的另一些有价值的函数，并研究当 A 在它所在的类中变化时这些

1) 在补充文献[1]中 (Theorem 6.8)，给出了 $\tilde{\rho} = \bar{\rho}$ 的一个充分必要条件．——译者注

函数的变化性状．这种研究已在某些场合付诸实施． 例如，若记规范类 $\mathfrak{A}$ 中矩阵的最小迹为 $\tilde{\sigma}$，最大迹为 $\bar{\sigma}$，则可以证明公式

$$\tilde{\sigma} = \max_{i,j}\{\min(i,j) - t_{ij}\} \quad (i = 0,1,\cdots,m; j = 0,1,\cdots,n) \tag{5.1}$$

和

$$\bar{\sigma} = \min_{i,j}\{t_{ij} + \max(i,j)\}$$
$$(i = 0, 1, \cdots, m; j = 0, 1, \cdots, n) \tag{5.2}$$

成立． 这些公式和 § 4 中 $\bar{\rho}$ 的公式很相似，而且也可循类似的途径来推导出这些公式．

但很多这类极值问题不能作这样彻底的处理．如设 A 属于规范类 $\mathfrak{A}(R, S)$，α 是满足 $1 \leqslant \alpha \leqslant r_m$ 的整数．设 E 是 A 的 $m \times \varepsilon$ 子矩阵，而且 E 的每行的行和不少于 α．使得这种 E 存在的最小正数 ε 称为 A 的 α-宽度，记作 $\varepsilon(\alpha)$． 现令 $\mathfrak{A}$ 中矩阵的最小 α-宽度为 $\tilde{\varepsilon}(\alpha)$，最大 α-宽度为 $\bar{\varepsilon}(\alpha)$． 可以证明，§ 1 中所构作的矩阵 $\tilde{A}$ 的 α-宽度是 $\tilde{\varepsilon}(\alpha)(\alpha = 1, 2, \cdots, r_m)$．事实上，$\tilde{A}$ 的最后一行中的第 α 个 1 在第 $\tilde{\varepsilon}(\alpha)$ 列． $\tilde{A}$ 的这个突出的性状给出了一个计算 $\tilde{\varepsilon}(\alpha)$ 的有效程序．但人们对 $\bar{\varepsilon}(\alpha)$ 的性状所知甚少．对此如能了解更多则极有价值，这到第八章就会明白，在那里我们将指出 $\bar{\varepsilon}(1)$ 和有限射影平面之间的相互联系．

某些特殊的类有一些本身很有价值的问题．记 $\mathfrak{A}(K, K)$ 是 $m = n$ 且

$$R = S = K = (k, k, \cdots, k) \tag{5.3}$$

的类．这里 k 是满足 $1 \leqslant k \leqslant n$ 的一个固定整数． 即 $\mathfrak{A}(K, K)$ 是所有在每一行和每一列上都正好有 k 个 1 的 n 阶 (0, 1)-矩阵的类． 当 $k = 1$ 时，这个类由 $n!$ 个 n 阶置换方阵组成，当 $k = n$ 时，则它由 n 阶方阵 J 组成．根据第五章的定理 5.3，可知对类 $\mathfrak{A}(K, K)$ 有

$$\tilde{\rho} = \bar{\rho} = m = n. \tag{5.4}$$

这时自然会进一步探求 $\mathfrak{A}(K, K)$ 中矩阵的最小积和式和最大积和式．但这两个值还不能确定．这个最小值可以具有相当深刻的组合意义，对双随机矩阵的相应问题便导致第五章的 van der

Waerden 猜想.

参 考 文 献

定理 1.1 由 Gale[9]和 Ryser[13] 得出. 定理 4.2 由 Haber[10] 得出. §2, §3, §4 的其余定理均取自 Ryser [12, 13, 14]. §3 的证明按照 Haber [10]. Haber[10,11] 讨论了最小项秩 $\tilde{\rho}$. Fulkerson[5] 和 Ryser[15] 研究了迹. Fulkerson 和 Ryser[6,7,8] 一起研究了 α-宽度.

[1] A. L. Dulmage and N. S. Mendelsohn, Coverings of bipartite graphs, *Canad, Jour. Math.*, **10** (1958), 517—534.

[2] ————, The term and stochastic ranks of a matrix, *Canad. Jour. Math.*, **11** (1959), 269—279.

[3] T. Evans, Embedding incomplete Latin squares, *Amer, Math. Monthly*, **67** (1960), 958—961.

[4] L. R. Ford, Jr. and D. R. Fulkerson, Flows in Networks, Princeton University Press, 1962.

[5] D. R. Fulkerson, Zero-one matrices with zero trace, *Pacific Jour. Math.*, **10** (1960), 831—836.

[6] D. R. Fulkerson and H. J. Ryser, Widths and heights of (0, 1)-matrices, *Canad, Jour. Math.*, **13** (1961), 239—255.

[7] ————, Multiplicities and minimal widths for (0, 1)-matrices, *Canad. Jour. Math.*, **14** (1962), 498—508.

[8] ————, Width sequences for special classes of (0, 1)-matrices, *Canad. Jour. Math.*, **15** (1963), 371—396.

[9] D. Gale, A theorem on flows in networks, *Pacific Jour. Math.*, **7** (1957), 1073—1082.

[10] R. M. Haber, Term rank of (0,1)-matrices, *Rend, Sem. Math. Padova*, **30** (1960), 24—51.

[11] ————, Minimal term rank of a class of (0,1)-matrices, *Canad. Jour. Math.*, **15** (1963), 188—192.

[12] H. J. Ryser, A combinatorial theorem with an application to Latin rectangles, *Proc. Amer. Math. Soc.*, **2** (1951), 550—552.

[13] ————, Combinatorial properties of matrices of zeros and ones, *Canad. Jour. Math.*, **9** (1957), 371—377.

[14] ————, The term rank of a matrix, *Canad. Jour. Math.*, **10** (1958), 57—65.

[15] ————, Traces of matrices of zeros and ones, *Canad. Jour. Math.*, **12** (1960), 463—476.

[16] ————, Matrices of zeros and ones, *Bull. Amer. Math. Soc.*, **66** (1960), 442—464.

译者补充文献

[1] R. A. Brualdi, Matrices of zeros and ones with fixed row and column sum vectors, *Linear Algebra and its Applications*, **33** (1980), 159—231.

第七章　正交拉丁方

§1. 存在定理

设 $A_1=[a_{ij}^{(1)}]$ 和 $A_2=[a_{ij}^{(2)}]$ 是两个在元素 $1,2,\cdots,n$ 上的 n 阶拉丁方 ($n\geqslant 3$). 如果 n^2 个 2-样品

$$(a_{ij}^{(1)},a_{ij}^{(2)})\qquad (i,j=1,2,\cdots,n)\tag{1.1}$$

互不相同,则称拉丁方 A_1 和 A_2 是正交的. 也可以这样定义: 如果把一个拉丁方叠置在另一个上,便得到一个由 $1,2,\cdots,n$ 的有序偶构成的 $n\times n$ 阵列, 这两个拉丁方正交相当于上述 $n\times n$ 阵列的 n^2 个元素互不相同. 由一对正交拉丁方的 2-样品构成的 $n\times n$ 阵列在文献中常被称作希腊-拉丁方或 Euler 方. 例如,

$$A_1=\begin{bmatrix}1&2&3\\2&3&1\\3&1&2\end{bmatrix},$$

$$A_2=\begin{bmatrix}1&2&3\\3&1&2\\2&3&1\end{bmatrix}\tag{1.2}$$

就是一对 3 阶正交拉丁方的实例.

更一般些,设 $A_1, A_2, \cdots, A_t$ 是一组 n 阶拉丁方, $n\geqslant 3$, $t\geqslant 2$. 如果只要 $i\neq j$, A_i 和 A_j 就正交,则称 $A_1, A_2, \cdots, A_t$ 是正交的,并把它们称为一个正交组. 我们在这一章中研究正交组. 这种组态由来已久,不过以前主要把它当作数学游戏. 而在今天,我们已认识到它们在研究有限射影平面以及其它课题上的重要性. 先从下列初等结果开始.

定理 1.1. 设 $A_1, A_2, \cdots, A_t$ 是 t 个 n 阶 ($n\geqslant 3$) 拉丁方的正交组,则

$$t\leqslant n-1.\tag{1.3}$$

证 我们分别对每个拉丁方的元素重新标号，使得这 t 个拉丁方的第一行元素从左到右都是 $1, 2\cdots, n$. 易见这样并不破坏这组拉丁方的正交性. 现在来观察这 t 个拉丁方在 $(2,1)$ 位置处的元素. 由正交性可知，这 t 个元素互不相同. 同时，它们又都不等于 1，所以 $t \leqslant n-1$.

如果在(1.3)式中等式成立，则称这个正交组是**完备的**. 前面的(1.2)是完备组.

这里我们预先假定读者知道一点有限域的初等性质. 所谓有限域，就是由有限个元素组成的域. 如记有限域的元素个数为 n，熟知必有 $n=p^\alpha$，这里 p 是素数，α 是正整数. 反过来，对每个素数 p 和每个正整数 α，一定存在一个有 $n=p^\alpha$ 个元素的域，而且两个元素个数相同的有限域一定同构. 有 $n=p^\alpha$ 个元素的域也叫 Galois 域，记为 $GF(p^\alpha)$. 如果 $\alpha=1$，$GF(p)$ 的元素可以取为模 p 的完全剩余组 $0, 1, \cdots, p-1$. 这时域的加法和乘法运算就是模 p 的普通加法和乘法. 现在我们证明一个完备正交拉丁方组的存在定理. 证明要用到 Galois 域 $GF(p^\alpha)$ 的存在性.

定理 1.2. 设 $n=p^\alpha$，其中 p 是素数，α 是正整数，则当 $n \geqslant 3$ 时，一定存在一个 $n-1$ 个 n 阶拉丁方的完备正交组.

证 记 Galois 域 $GF(p^\alpha)$ 的元素为 $a_0=0$，$a_1=1$，$a_2, \cdots, a_{n-1}$. 定义 $n-1$ 个 n 阶方阵

$$A_e=[a_{ij}^{(e)}]$$

$$(i, j=0, 1, \cdots, n-1; e=1, 2, \cdots, n-1), \quad (1.4)$$

其中

$$a_{ij}^{(e)}=a_e a_i+a_j. \quad (1.5)$$

先证式(1.4)中每个 A_e 都是拉丁方. 假如 A_e 在第 i 行上有两个相同元素，即有 j 和 j'，使

$$a_e a_i+a_j=a_e a_i+a_{j'}, \quad (1.6)$$

则必有 $a_j=a_{j'}$，从而 $j=j'$. 同样地，如果 A_e 在第 j 列上有两个相同元素，即有 i 和 i'，使

$$a_e a_i+a_j=a_e a_{i'}+a_j. \quad (1.7)$$

由于 $a_e \neq 0$，所以必有 $a_i = a_{i'}$，从而 $i = i'$，因此 A_e 是拉丁方．再证当 $1 \leqslant e < f \leqslant n - 1$ 时，A_e 和 A_f 正交．假设有

$$(a_{ij}^{(e)}, a_{ij}^{(f)}) = (a_{i'j'}^{(e)}, a_{i'j'}^{(f)}), \tag{1.8}$$

则

$$a_e a_i + a_j = a_e a_{i'} + a_{j'}, \tag{1.9}$$

$$a_f a_i + a_j = a_f a_{i'} + a_{j'}. \tag{1.10}$$

两式相减得

$$a_i(a_e - a_f) = a_{i'}(a_e - a_f). \tag{1.11}$$

因为 $a_e \neq a_f$，所以 $a_i = a_{i'}$，$i = i'$．以此代入(1.9)又得 $a_j = a_{j'}$，$j = j'$． 因此(1.4)是正交组．

定理 1.3. 对 $n \geqslant 3$ 和 $t \geqslant 2$，一个由 t 个 n 阶拉丁方组成的正交组，等价于一个 $n^2 \times (t+2)$ 阵列

$$A = [a_{ij}]$$

$$(i = 1, 2, \cdots, n^2;\ j = 1, 2, \cdots, t+2). \tag{1.12}$$

其中 A 的元素是 $1, 2, \cdots, n$，而且 A 的每一个 $n^2 \times 2$ 子阵列的 n^2 行表出了 $1, 2, \cdots, n$ 的全部 n^2 个 2-样品．

证　设有满足上述性质的阵列 A． 我们可对 A 作行的置换，使得由 A 所变成的阵列 B 的前两列所组成的 $n^2 \times 2$ 子阵列的第 1 到第 n^2 行元素排成自然顺序 $(1,1), (1,2), \cdots, (1,n), \cdots, (n,1), (n,2), \cdots, (n,n)$．这时，$B$ 的第 e 列 $(e = 3, 4, \cdots, t+2)$ 上的 n^2 个元素可按下法构成一个 $n \times n$ 阵列 B_e：B_e 的第 1 行由 B 的第 e 列的前 n 个元素组成，B_e 的第 2 行由 B 的第 e 列的第 $n+1$ 到第 $2n$ 这 n 个元素组成，一直到 B_e 的第 n 行由 B 的第 e 列的最后 n 个元素组成．如此作出的 $B_3, B_4, \cdots, B_{t+2}$ 一定是正交拉丁方组．事实上，由 B 的第 1 列的性质可知 B_e 的每一行上没有相同元素，由 B 的第 2 列的性质可知 B_e 的每一列上没有相同元素，所以 B_e 是拉丁方． 另外，如果 $e \neq f$，则由 B 的第 e 和第 f 两列构成的 $n^2 \times 2$ 子阵列的性质可知 B_e 和 B_f 正交．定理的另一半可类似地证明．

下面的阵列是与正交拉丁方组 (1.2) 相结合的：

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 3 & 3 & 3 \\ 2 & 1 & 2 & 3 \\ 2 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 1 & 3 \\ 3 & 3 & 2 & 1 \end{bmatrix}. \tag{1.13}$$

定理 1.4. 如果既存在 t 个 n 阶拉丁方的正交组，又存在 t 个 n' 阶拉丁方的正交组，则必存在 t 个 nn' 阶拉丁方的正交组.

证 我们按照定理 1.3，把 t 个 n 阶拉丁方的正交组和 n' 个拉丁方的正交组分别表为 $n^2 \times (t+2)$ 阵列 A 和 $n'^2 \times (t+2)$ 阵列 A'. 记 A 的第 i 行为

$$(a_{i1}, a_{i2}, \cdots, a_{i,t+2}), \tag{1.14}$$

记 A' 的第 j 行为

$$(a'_{j1}, a'_{j2}, \cdots, a'_{j,t+2}). \tag{1.15}$$

现在把(1.14)和(1.15)合成一个由 $t+2$ 个数偶组成的行

$$((a_{i1}, a'_{j1}), (a_{i2}, a'_{j2}), \cdots, (a_{i,t+2}, a'_{j,t+2})). \tag{1.16}$$

形如(1.16)的行共有 $(nn')^2$ 个，它们可以构成一个 $(nn')^2 \times (t+2)$阵列. 这个阵列的元素都是形如

$$(1,1),(1,2),\cdots,(1,n'),\cdots,(n,1),(n,2),\cdots,(n,n') \tag{1.17}$$

的数偶. 根据阵列 A 和 A' 的结构，可知这个阵列的每个 $(nn')^2 \times 2$ 子阵列的 $(nn')^2$ 行表出了 nn' 个元素(1.17)的全部 $(nn')^2$ 个 2-样品. 由定理 1.3，这个 $(nn')^2 \times (t+2)$ 阵列必能产生 t 个 nn' 阶拉丁方的正交组.

定理 1.5. 设正整数 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}$，其中 $p_1, p_2, \cdots, p_N$ 是互不相同的素数，α_i 是正整数. 又记

$$t = \min(p_i^{\alpha_i} - 1) \qquad (i = 1, 2, \cdots, N), \tag{1.18}$$

则对 $t \geq 2$，必存在 t 个 n 阶拉丁方的正交组.

证　根据定理 1.2，存在 t 个 $p_i^{r_i}$ 阶拉丁方的正交组．多次使用定理 1.4 即证定理 1.5．

这个定理说明，如果 $n \not\equiv 2 \pmod 4$，则一定存在一对 n 阶正交拉丁方．下一节研究当 $n \equiv 2 \pmod 4$ 时的 n 阶正交拉丁方组．

§2. Euler 猜想

Euler 提出下述 36 名军官的问题：有来自 6 个团队且分属 6 种军阶的 36 名军官，每个团队 6 名，每种军阶 6 名，问能否把这 36 名军官排成 6 行 6 列的方队，使得每行与每列的 6 名军官既有不同的军阶又来自不同的团队？我们用 1，2，3，4，5，6 把军阶和团队编号，这样每个军官可用 1 到 6 的一个 2-样品来代表，这个 2-样品的第 1 个分量表示该军官的军阶，第 2 个分量表示他所属的团队．Euler 的问题就归结为能否构作一对 6 阶正交拉丁方．Euler 在 1782 年猜想，不存在一对阶数 $n \equiv 2 \pmod 4$ 的正交拉丁方．Tarry 在 1900 年左右通过系统的枚举证实了当 $n = 6$ 时 Euler 猜想是正确的．但直到 1960 年左右，由 Bose, Shrikhande 和 Parker 的共同努力，才完全解决了 Euler 的猜想．他们得到下述定理：

定理 2.1.　设 $n \equiv 2 \pmod 4$，$n > 6$，则必存在一对 n 阶正交拉丁方．

这个定理表明实际情况和人们的期望相反，同时它也说明从不充分的根据飞跃到一般结论的危险．我们在这里不准备深入进行定理 2.1 的复杂的证明，但对定理2.1的一类特殊情况，我们给出一个简单精巧的构作．

定理 2.2.　设 $n \equiv 10 \pmod{12}$，则必存在一对 n 阶正交拉丁方．

证　假设有一对 m 阶正交拉丁方．对 $i = 0, 1, \cdots, 2m$，定义如下向量：

$$
\begin{aligned}
A_i &= (i, i, \cdots, i), \\
B_i &= (i+1, i+2, \cdots, i+m), \\
C_i &= (i-1, i-2, \cdots, i-m).
\end{aligned}
\tag{2.1}
$$

(2.1) 的每个向量都有 m 个分量，这些分量都看成是 $(\bmod 2m+1)$ 的整数. 从(2.1)我们再作差

$$
\begin{aligned}
D &= A_i - B_i \equiv (2m, 2m-1, \cdots, m+1), \\
D' &= B_i - A_i \equiv (1, 2, \cdots, m), \\
E &= A_i - C_i \equiv (1, 2, \cdots, m), \\
E' &= C_i - A_i \equiv (2m, 2m-1, \cdots, m+1), \\
F &= B_i - C_i \equiv (2, 4, \cdots, 2m), \\
F' &= C_i - B_i \equiv (2m-1, 2m-3, \cdots, 1). \\
& \qquad (\bmod\ 2m+1)
\end{aligned}
\tag{2.2}
$$

在(2.2)中，易见 D 和 D' 的全部 $2m$ 个分量是

$$1, 2, \cdots, 2m (\bmod 2m+1),$$

E 和 E'，F 和 F' 也一样. 这对 $i=0, 1, \cdots, 2m$ 都成立. 从向量 (2.1) 可以构作如下向量

$$
\begin{aligned}
A &= (A_0, A_1, \cdots, A_{2m}), \\
B &= (B_0, B_1, \cdots, B_{2m}), \\
C &= (C_0, C_1, \cdots, C_{2m}).
\end{aligned}
\tag{2.3}
$$

由式(2.2)可知

$$
\begin{aligned}
A - B &= (D, D, \cdots, D), \\
B - A &= (D', D', \cdots, D'), \\
A - C &= (E, E, \cdots, E), \\
C - A &= (E', E', \cdots, E'), \\
B - C &= (F, F, \cdots, F), \\
C - B &= (F', F', \cdots, F').
\end{aligned}
\tag{2.4}
$$

(2.3)和(2.4)式中每个向量都有 $m(2m+1)$ 个分量. 设

$$X = (x_1, x_2, \cdots, x_m) \tag{2.5}$$

是 m 个元素的一个排列. 从 X 可以构作 $m(2m+1)$-样品

$$Y = (X, X, \cdots, X). \tag{2.6}$$

从 A, B, C 和 Y 又可以构作 $4 \times 4m(2m+1)$ 阵列

$$G=\begin{bmatrix} A & B & C & Y \\ B & A & Y & C \\ C & Y & A & B \\ Y & C & B & A \end{bmatrix}. \quad (2.7)$$

对 G 的任一个 $2\times 4m(2m+1)$ 子阵列 G'，G' 一定含有下列子阵列之一：

$$\begin{bmatrix} A & Y \\ Y & A \end{bmatrix}, \begin{bmatrix} B & Y \\ Y & B \end{bmatrix}, \begin{bmatrix} C & Y \\ Y & C \end{bmatrix}. \quad (2.8)$$

根据 A，B，C 和 Y 的结构，这表明 G' 含有列

$$\begin{pmatrix} i \\ x_j \end{pmatrix}, \begin{pmatrix} x_j \\ i \end{pmatrix}, \quad (2.9)$$

其中 $i=0, 1, \cdots, 2m(\bmod 2m+1)$；$j=1, 2, \cdots, m$. 另外，$G'$ 一定含有下列子阵列之一：

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}, \begin{bmatrix} A & C \\ C & A \end{bmatrix}, \begin{bmatrix} B & C \\ C & B \end{bmatrix}. \quad (2.10)$$

如果 $i\neq j$，则 $i-j(\bmod 2m+1)$ 是 D 或 D' 的一个分量.同样它也是 E 或 E'，F 或 F' 的一个分量. 假如说，$i-j(\bmod 2m+1)$ 是 D 的一个分量，则它在 $A-B$ 中出现 $2m+1$ 次.$i-j(\bmod 2m+1)$ 在 $A-B$ 中第 $i+1$ 次出现时的位置正说明 (2.10) 式中的第 1 个阵列含有形如

$$\begin{pmatrix} i \\ j \end{pmatrix} \quad (2.11)$$

的一列.对其它情况有相类似的结论.所以 G' 一定含有列 (2.11)，这里 $i,j=0, 1, \cdots, 2m(\bmod 2m+1)$，$i\neq j$.

我们在证明的开始就假设了存在一对 m 阶正交拉丁方. 设 H 是 $4\times m^2$ 阵列，它是在 $x_1, x_2, \cdots, x_m$ 上的一对正交拉丁方按定理 1.3 所构作的 $m^2\times 4$ 阵列的转置阵列. 我们作阵列

$$Z=\begin{bmatrix} & & 0 & 1\cdots 2m \\ & & 0 & 1\cdots 2m \\ G & H & 0 & 1\cdots 2m \\ & & 0 & 1\cdots 2m \end{bmatrix}. \quad (2.12)$$

Z 的行数是 4，列数是

$$4m(2m+1)+m^2+2m+1=(3m+1)^2. \qquad (2.13)$$

Z 的每个 $2\times(3m+1)^2$ 子阵列的 $(3m+1)^2$ 列表出了 $x_1, x_2, \cdots, x_m$; $0, 1, 2, \cdots, 2m \pmod{2m+1}$ 这 $3m+1$ 元素的全部 $(3m+1)^2$ 个 2-样品．因此 Z 的转置是一个定理 1.3 所指出的那种 $(3m+1)^2\times 4$ 阵列．由定理 1.3 可知必存在一对 $n=3m+1$ 阶正交拉丁方．按定理 1.5，我们可取 $m\equiv 3 \pmod 4$，则 $n=3m+1\equiv 10 \pmod{12}$．$m$ 的其它选择所产生的值 $n=3m+1$ 都已包含在定理 1.5 的结果之中．

按上述构作可得如下一对 10 阶正交拉丁方：

$$A=\begin{bmatrix}
0 & 6 & 5 & 4 & x_3 & x_2 & x_1 & 1 & 2 & 3\\
x_1 & 1 & 0 & 6 & 5 & x_3 & x_2 & 2 & 3 & 4\\
x_2 & x_1 & 2 & 1 & 0 & 6 & x_3 & 3 & 4 & 5\\
x_3 & x_2 & x_1 & 3 & 2 & 1 & 0 & 4 & 5 & 6\\
1 & x_3 & x_2 & x_1 & 4 & 3 & 2 & 5 & 6 & 0\\
3 & 2 & x_3 & x_2 & x_1 & 5 & 4 & 6 & 0 & 1\\
5 & 4 & 3 & x_3 & x_2 & x_1 & 6 & 0 & 1 & 2\\
2 & 3 & 4 & 5 & 6 & 0 & 1 & x_1 & x_2 & x_3\\
4 & 5 & 6 & 0 & 1 & 2 & 3 & x_2 & x_3 & x_1\\
6 & 0 & 1 & 2 & 3 & 4 & 5 & x_3 & x_1 & x_2
\end{bmatrix},$$

$$B=\begin{bmatrix}
0 & x_1 & x_2 & x_3 & 1 & 3 & 5 & 2 & 4 & 6\\
6 & 1 & x_1 & x_2 & x_3 & 2 & 4 & 3 & 5 & 0\\
5 & 0 & 2 & x_1 & x_2 & x_3 & 3 & 4 & 6 & 1\\
4 & 6 & 1 & 3 & x_1 & x_2 & x_3 & 5 & 0 & 2\\
x_3 & 5 & 0 & 2 & 4 & x_1 & x_2 & 6 & 1 & 3\\
x_2 & x_3 & 6 & 1 & 3 & 5 & x_1 & 0 & 2 & 4\\
x_1 & x_2 & x_3 & 0 & 2 & 4 & 6 & 1 & 3 & 5\\
1 & 2 & 3 & 4 & 5 & 6 & 0 & x_1 & x_2 & x_3\\
2 & 3 & 4 & 5 & 6 & 0 & 1 & x_2 & x_1 & x_2\\
3 & 4 & 5 & 6 & 0 & 1 & 2 & x_3 & x_3 & x_1
\end{bmatrix}.$$

§3. 有限射影平面

现在我们开始研究有限射影平面．从表面上看，它与正交拉丁方完全没有联系．但我们在下一节将阐明这两个论题是密切相关的。所谓一个射影平面 π 是由一些称为"点"的元素和另一些称为"线"的元素组成的数学体系．这些点和线以"关联关系"结合在一起．也就是说，我们假定已定义了关系"点 P 在线 L 上"，或等价地，定义了关系"线 L 通过点 P"，而且这种关系满足下列公设：

(3.1) π 的两个不同的点在且仅在 π 的一条线上．

(3.2) π 的两条不同的线过且仅过 π 的一个点．

(3.3) π 上存在 4 个点，它们中的任意 3 点都不在同一线上．

公设(3.1)和(3.2)是最根本的．公设(3.3)用以排除一些只满足(3.1)和(3.2)的退化情况．从这三条公设可以推得下述的

(3.4) π 上有 4 条线，它们中的任意 3 条都不过同一点．

可以很清楚地看到，对有关射影平面的每个命题，只要在命题中把名词"点"和"线"互换，把句子"点 P 在线 L 上"和"线 L 过点 P"互换，都能得到其对偶命题．公设 (3.2)，(3.4) 就分别是公设(3.1)，(3.3)的对偶．这个"对偶原理"在射影平面的理论上是很重要的．

定理 3.1 设 P，P' 是射影平面 π 上两个不同的点，L，L' 是 π 上两条不同的线．则分别有 L 上的点的集合到 L' 上的点的集合之上的一一映射，通过点 P 的线的集合到通过点 P' 的线的集合之上的一一映射，以及 L 上的点的集合到通过 P 的线的集合之上的一一映射．

证　用记号 PQ 表示 π 上通过两个不同的点 P 和 Q 的唯一确定的线．我们先证 π 上必有一点 O，它既不在线 L 上，又不在线 L' 上．假如没有这样的点 O，则 π 上所有的点都在 L 或 L' 上．根据 (3.3)，必有点 A 和 B 在 L 上，点 C 和 D 在 L' 上，而且这 4 点 A，B，C，D 中任意 3 点都不在同一线上．而由此可知线 AC

和 BD 的交点既不在 L 上又不在 L' 上. 现在可以从既不在 L 上又不在 L' 上的点 O 出发来建立 L 上的点的集合到 L' 上的点的集合之上的一一映射：对 L 上任意一点 E,线 OE 与线 L' 相交于唯一确定的一点 E'. 这样建立一个把 E 映为 E' 的映射，易见这个映射是 L 上的点的集合到 L' 上的点的集合之上的一一映射. 定理中的第二个论断是上述结论的对偶命题. 又若 O 是不在 L 上的一点，易见有 L 上的点的集合到通过 O 的线的集合之上的一一映射. 根据定理的第二个一一映射的存在，当 O 在 L 上时上述断言也成立. 注意到我们通过上述证明已指出，π 的每一条线上至少有 3 个不同点,通过 π 的任一点至少有 3 条不同线.

只含有限个点的射影平面称为有限射影平面. 有限射影平面在组合数学中非常重要,在以下的讨论中它将起主要作用.如果在有限射影平面 π 的一条线 L 上总共有 $n+1$ 个点，则称正整数 n 为 π 的阶,它是 π 的基本不变量.

定理 3.2. 设 π 是 n 阶有限射影平面,则在 π 的每一条线上点的个数以及通过每一点的线的个数都是 $n+1$，而且 π 一共有 n^2+n+1 个点和 n^2+n+1 条线.

证　定理的前半部分是定理 3.1 和阶的定义的直接推论. 设 O 是 π 上一点,则正好有 $n+1$ 条线通过 O,而且每条线上除 O 之外正好还有 n 个点. 所以 π 上总共有 $1+n(n+1)=n^2+n+1$ 个点. 它的对偶命题断言 π 上总共有 n^2+n+1 条线.

n 阶有限射影平面还可以用别的等价的公设组来定义. 比方说，设 π 满足(3.2)和(3.3)，π 上共有 n^2+n+1 个点，每条线上正好有 $n+1$ 个点,过每点正好有 $n+1$ 条线,则 π 一定是 n 阶有限射影平面. 因为对 π 上一点 O,正好有 $n+1$ 条线通过 O,而每条线上除 O 之外正好还有 n 个点，所有这些点就是 π 上全部 n^2+n+1 个点. 从而 π 上一点 O 和另外一点在且仅在一条线上,这就证明了 (3.1),因此 π 是 n 阶有限射影平面.

最后我们指出,在很多场合,把 n 阶有限射影平面上的线当作点的 $(n+1)$-子集会比较方便. "最小"的射影平面是 2 阶的. 元

素 1, 2, ⋯, 7 的下列 7 个 3-子集展示了 2 阶射影平面上的 7 条线:

$$L_1 = \{1, 2, 4\},\quad L_2 = \{2, 3, 5\},\quad L_3 = \{3, 4, 6\},$$
$$L_4 = \{4, 5, 7\},\quad L_5 = \{5, 6, 1\},\quad L_6 = \{6, 7, 2\},$$
$$L_7 = \{7, 1, 3\}.$$

§4. 射影平面与拉丁方

在这一节，我们将建立有限射影平面与完备正交拉丁方组之间的联系.

定理 4.1. 设 $n \geqslant 3$. 可以构作 n 阶射影平面的充分必要条件是可以构作完备的 n 阶拉丁方的正交组.

证 假设已给出 n 阶射影平面 π. 设 L 是 π 上的一条线, P_1, $P_2, \cdots, P_{n+1}$ 是 L 上的 $n+1$ 个点. 记 π 上不在 L 中的其余 n^2 个点为 $Q_1, Q_2, \cdots, Q_{n^2}$. 对每个点 P_j, 我们把除 L 之外的通过 P_j 的 n 条线用 $1,2,\cdots,n$ 来编号(编号的方式可任意). 特别地,记 Q_iP_j 的编号为 a_{ij}. 这样得出一个在元素 $1,2,\cdots,n$ 上的 $n^2\times(n+1)$ 阵列

$$A = [a_{ij}]$$

$$(i = 1, 2, \cdots, n^2;\ j = 1, 2, \cdots, n+1). \tag{4.1}$$

我们说, A 的任一 $n^2 \times 2$ 子阵列的 n^2 行表出了 $1, 2, \cdots, n$ 的全部 n^2 个 2-样品. 假设不然,则有 $i \neq i'$, $j \neq k$, $a_{ij} = a_{i'j}$, $a_{ik} = a_{i'k}$. 亦即 $Q_iP_j = Q_{i'}P_j$, $Q_iP_k = Q_{i'}P_k$. 这说明 $Q_iQ_{i'}$ 既过 P_j 又过 P_k, 所以 $Q_iQ_{i'} = L$. 这与 Q_i 和 $Q_{i'}$ 都不在 L 上的假定矛盾. 所以 $n^2 \times (n+1)$ 阵列 A 是定理 1.3 所指出的那种阵列, 它能产生一个由 $n-1$ 个 n 阶拉丁方组成的正交组.

反过来,设有定理 1.3 所指出的那种阵列 (4.1). 记(4.1)的 n^2 行是 n^2 个"通常"点 $Q_1, Q_2, \cdots, Q_{n^2}$, 再用 $P_1, P_2, \cdots, P_{n+1}$ 表示 $n+1$ 个"理想"点. 一条"通常"线 L_{ij} 通过"理想"点 P_j 和阵列 (4.1) 中第 j 列元素等于 i 的那些行所代表的"通常"点. 一条"理想"线 L 通过所有"理想"点 $P_1, P_2, \cdots, P_{n+1}$. 这样我们定义了一个有 n^2+n+1 个点的组态 π. π 上每一点正好在 $n+1$ 条线

上，每条线正好通过 π 上 $n+1$ 个点．令 L_{ij} 和 $L_{i'k}$ 是两条"通常"线，且 $j \neq k$．它们有唯一公共点，这一点由(4.1)式中第 j 列元素等于 i，第 k 列元素等于 i' 的那一行所表示．令 L_{ij} 和 $L_{i'j}$ 是两条"通常"线，且 $i = i'$．它们有唯一公共点 P_j．"通常"线 L_{ij} 和"理想"线 L 的唯一公共点也是 P_j．以上证明了 π 满足 (3.2)．A 中第 1 第 2 两列元素分别是 (1,1),(1,2),(2,1),(2,2) 的 4 行所表示的 4 点满足(3.3)． 根据定理 3.2 的证明后面的说明，易见 π 是 n 阶有限射影平面．

定理 4.2. 设 $n = p^\alpha$，其中 p 是素数，α 是正整数，则必存在 n 阶有限射影平面．

证 $n = 2$ 时，已在前一节最后具体给出了 2 阶射影平面．$n \geq 3$ 时，本定理是定理 1.2 和定理 4.1 的推论．

设 n 是正整数，d 是能整除 n 的最大的平方数． 记 $n = n'd$，并称 n' 为 n 的**无平方因子部分**．如果 $d = 1$，则称 n 为**无平方因子的**．现在我们叙述关于有限射影平面的不存在性的 Bruck-Ryser 定理．

定理 4.3. 当 $n \equiv 1$ 或 $2 \pmod 4$ 且 n 的无平方因子部分至少有一个素因子 $p \equiv 3 \pmod 4$ 时，n 阶有限射影平面不存在．

我们将在第八章中证明定理 4.3 的推广．显然，定理 4.3 排除了无数种有限射影平面的存在．例如，当 $n = 2p$，p 是素数而且 $p \equiv 3 \pmod 4$ 时，就不存在 n 阶射影平面．当然，定理 4.2 和定理 4.3 留下了无数个待定的 n．实际上迄今为止，除了定理 4.2 和定理 4.3 所指出的 n 的那些值之外，对其余的值 n，n 阶射影平面的存在与否都还是不确定的．对此形成了两种对立观点：有人认为只有当 $n = p^\alpha$ 时才存在 n 阶射影平面；另外一部分人认为，只要不是定理 4.3 所指出的 n，就一定存在 n 阶射影平面． 确定 n 的精确范围是当今组合数学中主要的未解决的问题之一．第一个未解决情况是 $n = 10$．存在 10 阶射影平面要求构作 9 个 10 阶拉丁方的正交组，但还没有人能作出 3 个正交的 10 阶拉丁方．

参 考 文 献

MacNeish[8] 和 Mann[9] 讨论了 § 1 的内容. 关于 Euler 猜想的基本文献有 Bose 和 Shrikhande[2, 3], Parker[11, 12]. 定理 2.2 的论证根据 Bose, Shrikhande 和 Parker[4]. Tarry[18] 解决了 $n=6$ 的情形. 定理 4.1 根据 Bose[1]和 Stevens[17]; 定理 4.2 根据 Veblen 和 Bussey[19]; 定理 4.3 根据 Bruck和 Ryser[5].

[1] R. C. Bose, On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares, *Sankhyā*, 3 (1938), 323—338.

[2] R. C. Bose and S. S. Shrikhande, On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order 4t+2, *Proc. Nat. Acad. Sci. U. S. A.*, **45** (1959), 734—737.

[3] R. C. Bose and S. S. Shrikhande, On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Trans. Amer. Math. Soc.*, **95** (1960), 191—209.

[4] R. C. Bose, S. S. Shrikhande and E. T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. Jour. Math.*, **12** (1960), 189—203.

[5] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canad. Jour. Math.*, **1** (1949), 88—93.

[6] M. Hall, Jr., Projective planes, *Trans. Amer. Math. Soc.*, **54** (1943), 229—277.

[7] ————, Projective Planes and Related Topics, California Institute of Technology, 1954.

[8] H. F. MacNeish, Euler squares, *Ann. Math.*, **23** (1922), 221—227.

[9] H. B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Stat.*, **13** (1942), 418—423.

[10] ————, On orthogonal Latin squares, *Bull. Amer. Math. Soc.*, **50** (1944), 249—257.

[11] E. T. Parker, Construction of some sets of mutually orthogonal Latin squares, *Proc. Amer. Math. Soc.*, **10** (1959), 946—949.

[12] ————, Orthogonal Latin squares, *Proc. Nat. Acad. Sci., U. S. A.*, **45** (1959), 859— 862.

[13] ————, Nonextendibility conditions on mutually orthogonal Latin squares, *Proc. Amer. Math. Soc.*, **13** (1962), 219—221.

[14] G. Pickert, Projective Ebenen, Berlin, Springer-Verlag, 1955.

[15] H. J. Ryser, Geometries and incidence matrices, *Slaught Memorial Papers, no.* 4 (1955), 25—31.

[16] L. A. Skornyakov Projective planes, Mmer. Math. Soc., translation no. 99, 1953.

[17] W. L. Stevens, The completely orthogonalized Latin square, *Ann. Eugen.*, **9** (1939), 82—93.

[18] G. Tarry, Le problème de 36 officieurs, *Compte Rendu de L' Association Française pour L' Avancement de Science Naturel.* **1** (1900), 122—123, **2** (1901), 170—203.

[19] O. Veblen and W. H. Bussey, Finite projective geomertices, *Trans. Amer. Math. Soc.*, 7 (1906), 241—259.

第八章 组合设计

§1. (b, v, r, k, λ)-组态

我们在这一节引入的组合组态，是第七章所讨论的有限射影平面的推广．设X是元素为$x_1, x_2, \cdots, x_v$的v-集，$X_1, X_2, \cdots, X_b$是X的b个不同的子集．假设这些子集满足下列条件：

(1.1)每个X_i是X的k-子集，

(1.2)X的每个2-子集正好是b个集合$X_1, X_2, \cdots, X_b$中λ个集合的子集，

(1.3)整数v, k和λ满足$0 < \lambda, k < v-1$.

则称这些子集是一个平衡不完全区组设计．

在上述平衡不完全区组设计的定义中，条件(1.1)和(1.2)是基本的，条件(1.3)用来排除某些退化情况．统计学中有一个分支叫做试验的分析和设计．平衡不完全区组设计在这一分支中极为重要．在统计学中元素称为品种(varieties)，集合称为区组(blocks)，所以我们分别使用了字母v和b．设$x \in X$，并设x正好属于b个子集$X_1, X_2, \cdots, X_b$中的r个．现考察X的含x的$v-1$个2-子集．(1.1)和(1.2)都能用来确定这$v-1$个2-子集在b个集合$X_1, X_2, \cdots, X_b$中出现的次数．用(1.1)算得这个次数是$r(k-1)$，用(1.2)算得$\lambda(v-1)$．所以有

$$r(k-1) = \lambda(v-1). \tag{1.4}$$

上式告诉我们，r也是平衡不完全区组设计的一个不变量．它是一个元素在子集$X_1, X_2, \cdots, X_b$中出现的次数，也称重复数．由于v个元素的每一个的重复数都是r，而每个子集X_i都是X的k-子集，所以

$$bk = vr. \tag{1.5}$$

一个平衡不完全区组设计含有5个基本参数b, v, r, k和λ,

所以今后我们把它称为一个(b, v, r, k, λ)-组态，这5个整数不是互相无关的，它们用(1.4)和(1.5)式相联系. 不过(1.4)和(1.5)式对于存在一个(b, v, r, k, r)-组态来讲并不充分. 事实上，确定能使组态存在的b, v, r, k和λ的值的精确范围是研究这种组态的中心问题. 这个问题当然没有完全解决，而它的某些特殊情形就其本身来讲是十分重要的.

现设

$$A = [a_{ij}] \qquad (i = 1, 2, \cdots, b; j = 1, 2, \cdots, v) \tag{1.6}$$

是(b, v, r, k, λ)-组态的关联矩阵. 也就是说，A是$b \times v$的(0, 1)-矩阵. 当$x_j \in X_i$时，$a_{ij} = 1$；否则$a_{ij} = 0$. 由(b, v, r, k, λ)-组态的基本性质可以推出

$$AJ = kJ', \tag{1.7}$$

$$A^T A = (r - \lambda)I + \lambda J. \tag{1.8}$$

这里A^T是A的转置，J是元素全是1的v阶方阵，J'是元素全是1的$b \times v$矩阵，I是v阶单位方阵. 反过来，如果$0 < \lambda, k < v - 1$，而A是满足(1.7)和(1.8)式的$b \times v$的(0,1)-矩阵，则一定存在(b, v, r, k, λ)-组态，它的关联矩阵等于A.

如果我们把一个(0,1)-矩阵中的1改成0，0改成1，这样得到的新(0,1)-矩阵称为原矩阵的补. 若A是一个(b, v, r, k, λ)-组态的关联矩阵，A'是A的补. 不难验证，A'满足

$$A'J = k'J', \tag{1.9}$$

$$A'^T A' = (r' - \lambda')I + \lambda' J. \tag{1.10}$$

这里$r' = b - r, k' = v - k, \lambda' = b - 2r + \lambda$. 再用(1.4)和(1.5)可得$(b - r)(v - k - 1) = \lambda'(v - 1)$. 所以，如果$0 < \lambda, k < v - 1$，则$0 < \lambda', k' < v - 1$. 也就是说，$A'$定义了一个$(b, v, r', k', \lambda')$-组态. 我们把$A'$所定义的$(b, v, r', k', \lambda')$-组态称为$A$所定义的$(b, v, r, k, \lambda)$-组态的补.

设A_1，A_2是两个(b, v, r, k, λ)-组态的关联矩阵. 如果有b阶置换方阵P和v阶置换方阵Q，使

$$A_1 = PA_2Q \tag{1.11}$$

成立，则称这两个组态是同构的．对于取定的一组参数 b, v, r, k, λ 来讲，同构的 (b, v, r, k, λ)-组态可以不加区别，因为同构的两个组态只是元素以及子集的标号不同而已．

关联矩阵给我们提供了一个研究(b, v, r, k, λ)-组态的有力手段．这点可用下述定理来说明，它使用关联矩阵导出 Fisher 的一个不等式．

定理 1.1. (b, v, r, k, λ)-组态一定有 $b \geqslant v$.

证　设 A 是 (b, v, r, k, λ)-组态的关联矩阵．则 A 是 $b \times v$ 的(0,1)-矩阵．如果 $b < v$，我们可以添加 $v-b$ 行 0 到 A 上，得到一个 v 阶(0,1)-方阵 A^*．这时 A^* 一定满足

$$A^{*T}A^* = (r-\lambda)I + \lambda J. \tag{1.12}$$

我们现在用两种方法计算 $\det(A^{*T}A^*)$．一方面，由于 A^* 有一行全为 0，所以 $\det(A^{*T}A^*) = \det(A^{*T})\det(A^*) = 0$．另一方面，$v$ 阶方阵 $(r-\lambda)I + \lambda J$ 的主对角线上是 r，其余地方都是 λ．不难算出

$$\det((r-\lambda)I + \lambda J) = (r + (v-1)\lambda)(r-\lambda)^{v-1}. \tag{1.13}$$

所以 $\det(A^{*T}A^*) \neq 0$．因此不可能 $b < v$，即一定有 $b \geqslant v$.

根据(1.4)和(1.5)，当 $k = 2, \lambda = 1$ 时，一个 (b, v, r, k, λ)-组态有 $b = v(v-1)/2$，$r = v-1$．所以这种组态是一个 v-集的所有 2-子集的集合．$k = 3, \lambda = 1$ 时组态的意义更大．设 X 是 v-集，$v \geqslant 3$．所谓一个 v 阶 Steiner 三连系，是指 X 的一些 3-子集(或称三连)的集合，它使 X 的每个 2-子集正好是一个三连的子集．下面分别列举了阶数是 3, 7, 9 的 Steiner 三连系．

$(v=3)$　$\{1, 2, 3\}$.

$(v=7)$　$\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}$,
$\{5,6,1\}, \{6,7,2\}, \{7,1,3\}$.

$(v=9)$　$\{1,2,3\}, \{4,5,6\}, \{7,8,9\}$,
$\{1,4,7\}, \{2,5,8\}, \{3,6,9\}$,
$\{1,5,9\}, \{2,6,7\}, \{3,4,8\}$,
$\{1,6,8\}, \{2,4,9\}, \{3,5,7\}$.

注意到7阶 Steiner 三连系正是上一章提到的2阶射影平面。易见阶数 $v>3$ 的 Steiner 三连系就是 $k=3$，$\lambda=1$ 时的 (b,v,r,k,λ)-组态。因此由(1.4)和(1.5)式可得

$$b=v(v-1)/6,\quad r=(v-1)/2. \tag{1.14}$$

根据(1.14)式，一个 Steiner 三连系的阶 $v\geqslant 3$，$v\equiv 1$ 或 $3(\mathrm{mod}\,6)$。对所有这些 v 的值，v 阶 Steiner 三连系都已作出。Reiss 早在1859年就进行了这种构作，以后又继续得到许多进一步的结果。当 $v=3,7,9$ 时，三连系是唯一的。有2个13阶三连系，有80个15阶三连系。当 $v>15$ 时，还不知道究竟有多少个 v 阶三连系。这里我们只提出下述初等构作。

定理 1.2. 如果分别有 v_1 阶和 v_2 阶的 Steiner 三连系 S_1 和 S_2，则有 v_1v_2 阶的 Steiner 三连系 S。

证 设三连系 S_1 和 S_2 中的三连分别是 v_1-集 $\{a_1,a_2,\cdots,a_{v_1}\}$ 和 v_2-集 $\{b_1,b_2,\cdots,b_{v_2}\}$ 的3-子集。我们作一个 v_1v_2-集，其元素为 $c_{ij}(i=1,2,\cdots,v_1;\ j=1,2,\cdots,v_2)$，同时规定当 $\{c_{ir},c_{js},c_{kt}\}$ 符合以下三种情况之一时方属于 S：(1) $r=s=t$，$\{a_i,a_j,a_k\}\in S_1$，(2) $i=j=k$，$\{b_r,b_s,b_t\}\in S_2$，(3) $\{a_i,a_j,a_k\}\in S_1$，$\{b_r,b_s,b_t\}\in S_2$。不难验证如此定义的 S 确实是 v_1v_2 阶的 Steiner 三连系，S 中形如 $\{c_{i1},c_{j1},c_{k1}\}$ 的三连的集合与 S_1 同构；形如 $\{c_{1r},c_{1s},c_{1t}\}$ 的三连的集合与 S_2 同构。

设 n 是非负整数。一个阶数 $v=6n+3$ 的 Steiner 三连系如果再满足下述附加条件，就称为一个阶数 $v=6n+3$ 的 Kirkman 三连系。附加条件是：这个 Steiner 三连系中 $b=(2n+1)(3n+1)$ 个三连的集合可以划分成 $3n+1$ 部份，每部份都含有 $2n+1$ 个三连，而且 $v=6n+3$ 个元素中的每一个在以上 $3n+1$ 部份中正好出现一次。3阶 Steiner 三连系是退化的，即 $n=0$ 时的 Kirkman 三连系，前面列出的9阶 Steiner 三连系是 $n=1$ 时的 Kirkman 三连系。这时12个三连划分成四部分，这四部分就是前面列出的4行。易见9个元素中的每一个在每一行中正好出现一次。

Kirkman 的著名的 15 名女生问题可以陈述如下：一位教员每天组织她班上的 15 名女生散步．散步时女生排成 5 行，每行 3 人，使每个女生有两个同伴．问能否连续组织 7 次散步，使每 2 名女生至多只有一次排在同一行？这个问题等价于构作一个 $n=2$ 时的 Kirkman 三连系．下列三连系就是：

$\{1,2,5\}$，$\{3,14,15\}$，$\{4,6,12\}$，$\{7,8,11\}$，$\{9,10,13\}$，
$\{1,3,9\}$，$\{2,8,15\}$，$\{4,11,13\}$，$\{5,12,14\}$，$\{6,7,10\}$，
$\{1,4,15\}$，$\{2,9,11\}$，$\{3,10,12\}$，$\{5,7,13\}$，$\{6,8,14\}$，
$\{1,6,11\}$，$\{2,7,12\}$，$\{3,8,13\}$，$\{4,9,14\}$，$\{5,10,15\}$，
$\{1,8,10\}$，$\{2,13,14\}$，$\{3,4,7\}$，$\{5,6,9\}$，$\{11,12,15\}$，
$\{1,7,14\}$，$\{2,4,10\}$，$\{3,5,11\}$，$\{6,13,15\}$，$\{8,9,12\}$，
$\{1,12,13\}$，$\{2,3,6\}$，$\{4,5,8\}$，$\{7,9,15\}$，$\{10,11,14\}$．

§2. (v,k,λ)-组态

设 X 是元素为 $x_1, x_2, \cdots, x_v$ 的 v-集，$X_1, X_2, \cdots, X_v$ 是 X 的子集．如果这些子集满足下列条件：

每个 X_i 是 X 的 k-子集，　　(2.1)

$i\neq j$ 时，$X_i\cap X_j$ 都是 X 的 λ-子集，　　(2.2)

整数 v, k, λ 满足 $0<\lambda<k<v-1$．　　(2.3)

则称这些子集为一个 (v,k,λ)-**组态**．

设

$$A=[a_{ij}]\qquad (i,j=1,2,\cdots,v) \tag{2.4}$$

是 (v,k,λ)-组态的关联矩阵，则 A 是 v 阶 (0,1) -方阵．同时由 (2.1) 和 (2.2) 可得

$$AA^T=B=(k-\lambda)I+\lambda J. \tag{2.5}$$

这里 A^T 是 A 的转置，J 是元素全是 1 的 v 阶方阵，I 是 v 阶单位方阵．反过来，如果 $0<\lambda<k<v-1$，而 A 是满足(2.5) 的 v 阶 (0,1)-方阵，则一定存在 (v,k,λ)-组态，它的关联矩阵等于 A．

如果一个元素是实数的方阵 M 满足 $MM^T=M^TM$，则称 M 是**正规**方阵．我们有如下结果．

定理 2.1. (v,k,λ)-组态的关联矩阵 A 是正规的．从而有

$$AA^T = A^TA = B. \tag{2.6}$$

证　设 A 是 (v,k,λ)-组态的关联矩阵．由 (1.13) 可知

$$\det(B) = (k+(v-1)\lambda)(k-\lambda)^{v-1}. \tag{2.7}$$

因此 $\det(AA^T)=\det(A)\det(A^T) = \det(B) \neq 0$，从而 $\det(A) \neq 0$．记 A 的逆方阵为 A^{-1}．由于 $AJ = kJ$，所以 $A^{-1}J = k^{-1}J$．另外还有

$$AA^TJ = BJ = (k-\lambda+\lambda v)J \tag{2.8}$$

和

$$A^TJ = (k-\lambda+\lambda v)k^{-1}J. \tag{2.9}$$

对 (2.9) 式两边取转置后得到

$$JA = (k-\lambda+\lambda v)k^{-1}J. \tag{2.10}$$

所以

$$JAJ = (k-\lambda+\lambda v)k^{-1}vJ. \tag{2.11}$$

但又有

$$JAJ = kvJ, \tag{2.12}$$

所以由(2.11),(2.12)得到

$$k-\lambda = k^2-\lambda v. \tag{2.13}$$

把(2.13)代入到(2.10)中后得到

$$JA = kJ. \tag{2.14}$$

最后可计算出

$$\begin{aligned} A^TA &= A^{-1}(AA^T)A = A^{-1}BA = (k-\lambda)I + \lambda A^{-1}JA \\ &= (k-\lambda)I + \lambda J = B. \end{aligned} \tag{2.15}$$

定理证毕．

定理 2.2. 一个 (v,k,λ)-组态等价于一个当 $b=v, r=k$ 时的 (b,v,r,k,λ)-组态．

证　这是定理 2.1 的直接推论．

在统计学中，(v,k,λ)-组态称为对称平衡不完全区组设计．这种组态在纯粹和应用数学的很多领域中都会碰到，本章余下的部分就来研究这种组态．

定理 2.3. 一个 n 阶有限射影平面等价于一个参数 $v=n^2+n+1$, $k=n+1$ 和 $\lambda=1$ 的 (v, k, λ)-组态.

证 这是第七章 § 3 的结论和本章定理 2.1 的推论.

在第七章里,我们证明了 $n=p^\alpha$ 阶射影平面的存在,这里 p 是素数, α 是正整数. 我们也指出,迄今为止能构作的也只有这种阶是素数幂的有限射影平面. 还知道阶等于 2, 3, 4, 5, 7 或 8 的射影平面是唯一的. 但不知道当 $n>8$, $n=p^\alpha$ 时 n 阶射影平面的个数.

我们现在研究另一类重要的 (v, k, λ)-组态. 为此,先引入 Hadamard 矩阵的概念. 所谓 n 阶 Hadamard 矩阵 H, 是指一个 n 阶方阵 H, H 的元素是 $+1$ 或 -1, 同时 H 还满足方程

$$HH^T=nI, \tag{2.16}$$

这里 H^T 是 H 的转置, I 是 n 阶单位方阵. 由(2.16)易得

$$\det(H)\text{的绝对值}=n^{\frac{n}{2}}. \tag{2.17}$$

我们顺便指出, Hadamard 矩阵是从下列问题中很自然地产生的:如果一个方阵的元素都是绝对值不超过 1 的实数,则著名的 Hadamard 不等式断言这个方阵的行列式的绝对值不超过 $n^{\frac{n}{2}}$. 而且还可以证明,当且仅当方阵是 Hadamard 矩阵时才达到 $n^{\frac{n}{2}}$.

由矩阵方程(2.16)可知, H 的逆方阵是

$$H^{-1}=n^{-1}H^T. \tag{2.18}$$

所以 H 一定是正规的,而且

$$HH^T=H^TH=nI. \tag{2.19}$$

如果我们用 -1 乘 Hadamard 矩阵的某一行或某一列,则仍得 Hadamard 矩阵. 因此,我们总可以通过这种方法使一个 Hadamard 矩阵的第 1 行和第 1 列全变成 $+1$. 这种 Hadamard 矩阵称为规范化的. 1 阶、2 阶的规范化 Hadamard 矩阵是

$$[1], \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

对于阶数 $n\geqslant 3$ 的规范化 Hadamard 矩阵,根据 (2.16), 可知每一

行上 +1 和 −1 各一半，因此可以作列的置换，使第二行上前 $\frac{n}{2}$ 个元素是 +1，后 $\frac{n}{2}$ 个元素是 −1. 记第 3 行上前 $\frac{n}{2}$ 个位置中有 t 个 +1，后 $\frac{n}{2}$ 个位置中有 t' 个 +1. 同样根据 (2.16) 可得 $2t + 2t' = n, 2t - 2t' = 0$. 所以 $n = 4t$. 这表明 Hadamard 矩阵的阶数 n 一定是 1,2 或 $n \equiv 0 \pmod 4$.

人们猜想所有阶数 $n \equiv 0 \pmod 4$ 的 Hadamard 矩阵都存在. 为了构作这种矩阵，提出了不少有效的方法. 例如，对 $n \equiv 0 \pmod 4$，同时 $n \leqslant 200$ 的所有 n 阶 Hadamard 矩阵，除 $n = 116, 156, 168$ 外都已作出[1]. 以下我们只讲一种很简单的构作方法.

设 $A = [a_{ij}]$ 和 $A' = [a'_{ij}]$ 分别是 n 阶和 n' 阶方阵，它们的元素都在域 F 中. 我们定义 nn' 阶方阵

$$A \times A' = \begin{bmatrix} a_{11}A' & a_{12}A' & \cdots & a_{1n}A' \\ a_{21}A' & a_{22}A' & \cdots & a_{2n}A' \\ \vdots & \vdots & & \vdots \\ a_{n1}A' & a_{n2}A' & \cdots & a_{nn}A' \end{bmatrix} \tag{2.20}$$

为 A 和 A' 的直积.

定理 2.4. 两个 Hadamard 矩阵的直积仍是 Hadamard 矩阵.

证 设 H 和 H' 分别是 n 阶和 n' 阶 Hadamard 矩阵. 我们可以直接检验 $H \times H'$ 的行的内积确实满足 Hadamard 矩阵的条件. 也可以利用直积运算的一些性质作如下推导:

$$\begin{aligned}(H \times H')(H \times H')^T &= (H \times H')(H^T \times H'^T) \\ &= HH^T \times H'H'^T = nI_n \times n'I_{n'} = nn'I_{nn'},\end{aligned} \tag{2.21}$$

这里 I_n, $I_{n'}$ 和 $I_{nn'}$ 分别记 n 阶，n' 阶和 nn' 阶单位方阵. 注意到根据这个定理，我们已证明了所有阶数 $n = 2^a$ 的 Hadamard 矩阵都一定存在.

我们现在来建立 Hadamard 矩阵和 (v, k, λ)-组态之间的联

---

1) 现 116 和 156 阶 Hadamard 矩阵已作出. ——译者注

系．

定理 2.5. 一个阶数 $n=4t\geqslant 8$ 的规范化 Hadamard 矩阵等价于一个参数为 $v=4t-1, k=2t-1, \lambda=t-1$ 的 (v,k,λ)-组态．

证 设H是一个n阶规范化 Hadamard 矩阵，$n=4t\geqslant 8$. 我们去掉H的第 1 行和第 1 列，再在余下的$n-1$阶方阵中把 -1 都换成 0．这样得出一个v阶(0,1)-矩阵 A, $v=4t-1$. 由于H是规范化 Hadamard 矩阵，所以A一定满足矩阵方程

$$AA^{T}=tI+(t-1)J. \tag{2.22}$$

从而A是一个参数为 $v=4t-1$, $k=2t-1$, $\lambda=t-1$ 的(v, k, λ)-组态的关联矩阵．以上整个论证是可逆的．所以从一个参数为 $v=4t-1, k=2t-1, \lambda=t-1$ 的 (v,k,λ)-组态的关联矩阵A出发，也可以构作一个 $n=4t$ 阶的规范化 Hadamard 矩阵．

参数为 $v=4t-1$, $k=2t-1$, $\lambda=t-1$ 的 (v, k, λ)-组态的补是一个参数为 $v=4t-1$, $k'=2t$, $\lambda'=t$ 的 (v, k', λ')-组态．我们把这两种组态都称作 Hadamard 组态．可以指出一个有意义的事实：$v=7, k=3, \lambda=1$ 的 (v, k, λ)-组态在这里起着特殊的作用，它同时是 Steiner 三连系、有限射影平面和 Hadamard 组态．

§3. 一个不存在定理

我们先作一些准备性的说明．设 $S=[s_{ij}]$ 和 $S'=[s'_{ij}]$ 都是元素在域F中的n阶对称方阵．如果存在域F上的n阶可逆方阵P，使

$$P^{T}SP=S', \tag{3.1}$$

其中 P^{T} 是P的转置，则我们称S和 S' 在F上**相合**，记为 $S\overset{c}{=}S'$. 容易验证方阵的相合是一种等价关系．即相合关系满足 $S\overset{c}{=}S$; $S\overset{c}{=}S'$ 蕴涵 $S'\overset{c}{=}S$; $S\overset{c}{=}S'$ 和 $S'\overset{c}{=}S^{*}$ 蕴涵 $S\overset{c}{=}S^{*}$.

仍设 $S=[s_{ij}]$ 是域F上的n阶对称方阵，又

$$f = f(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} x_i s_{ij} x_j \qquad (3.2)$$

是未定元 $x_1, x_2, \cdots, x_n$ 的一个二次型. 我们称 f 为方阵 S 的**二次型**.
若 $S' = [s'_{ij}]$ 是域 F 上的另一个 n 阶对称方阵, 而且在 F 上 $S \overset{c}{=} S'$, 则有 F 上的非异方阵 $P = [p_{ij}]$, 使 $P^T SP = S'$. 现在设 $y_1, y_2, \cdots, y_n$ 是另一组未定元, 而且有

$$x_i = \sum_{j=1}^{n} p_{ij} y_j \qquad (i = 1, 2, \cdots, n). \qquad (3.3)$$

由于 P 可逆, 记 $P^{-1} = Q = [q_{ij}]$, 则 (3.3) 式等价于

$$y_i = \sum_{j=1}^{n} q_{ij} x_j \qquad (i = 1, 2, \cdots, n). \qquad (3.4)$$

如果我们把(3.3)代入(3.2), 则得未定元 $y_1, y_2, \cdots, y_n$ 的一个二次型 f'. 可以直接算得

$$f' = f'(y_1, y_2, \cdots, y_n) = \sum_{i,j=1}^{n} y_i s'_{ij} y_j. \qquad (3.5)$$

也就是说, f' 是方阵 S' 的二次型. 称二次型 f 和 f' 在 F 上相合.
由以上记号可知, 如果 $x'_1, x'_2, \cdots, x'_n$ 是 F 中任意 n 个元素, 而且

$$y'_i = \sum_{j=1}^{n} q_{ij} x'_j \qquad (i = 1, 2, \cdots, n), \qquad (3.6)$$

则在 F 中等式

$$f(x'_1, x'_2, \cdots, x'_n) = f'(y'_1, y'_2, \cdots, y'_n) \qquad (3.7)$$

成立. 同样, 如果 $y^*_1, y^*_2, \cdots, y^*_n$ 是 F 中任意 n 个元素, 而且

$$x^*_i = \sum_{j=1}^{n} p_{ij} y^*_j \qquad (i = 1, 2, \cdots, n), \qquad (3.8)$$

则在 F 中

$$f(x^*_1, x^*_2, \cdots, x^*_n) = f'(y^*_1, y^*_2, \cdots, y^*_n) \qquad (3.9)$$

也成立.

假设 A 和 A' 分别是域 F 上的 n 阶和 n' 阶方阵. 我们定义 $n + n'$ 阶方阵

$$A \dotplus A' = \begin{bmatrix} A & 0 \\ 0 & A' \end{bmatrix} \tag{3.10}$$

为 A 和 A' 的直和. 上式中 0 表示元素全是 0 的矩阵. 如果

$$S_1 \overset{c}{=} S_1', \quad S_2 \overset{c}{=} S_2',$$

则易见

$$S_1 \dotplus S_2 \overset{c}{=} S_1' \dotplus S_2'. \tag{3.11}$$

方阵相合理论的复杂性在很大程度上取决于所在的域的性质. Sylvester 的经典工作解决了实数域上的方阵相合问题,这时并不特别困难. 但有理数域的情形要复杂得多, 因为这时所论问题与数论的很多深刻问题密切相关. 我们现在对有理数域上的相合作少许初等说明.

设 m 是正整数, 根据 Lagrange 定理, m 必可表为 4 个整数 a_1, a_2, a_3, a_4 的平方和

$$m = a_1^2 + a_2^2 + a_3^2 + a_4^2. \tag{3.12}$$

对我们的讨论来讲,只要知道这 4 个数是有理数就够了. 用 I_n 记 n 阶单位方阵,定义

$$H = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & -a_1 & a_4 & -a_3 \\ a_3 & -a_4 & -a_1 & a_2 \\ a_4 & a_3 & -a_2 & -a_1 \end{bmatrix}. \tag{3.13}$$

根据 (3.12),由直接计算可得

$$HH^T = mI_4, \tag{3.14}$$

所以在有理数域上有

$$mI_4 \overset{c}{=} I_4. \tag{3.15}$$

根据 (3.11),由此可得

$$mI_n \overset{c}{=} I_n \tag{3.16}$$

对所有 $n \equiv 0 \pmod 4$ 成立.

我们回到关于 (v, k, λ)-组态的讨论. 这种组态的研究的中心问题是确定使组态存在的 v, k 和 λ 的值的精确范围. 按照定

义，v，k，λ 是满足 $0<\lambda<k<v-1$ 的整数．同时，由(2.13)式可知

$$k-\lambda=k^2-\lambda v. \tag{3.17}$$

这些都是使 (v, k, λ)-组态存在的必要条件．当我们讨论 (v, k, λ)-组态的存在时，总假定其参数 v，k，λ 满足这些必要条件．下述定理给出另一个必要条件．此外就不知道再有其它必要条件．所以人们猜想，除下述定理所特别排除的情形外，对所有其余的 v，k，λ 的值，(v, k, λ)-组态都存在．

定理 3.1. 设 v，k，λ 是整数，而且存在一个 (v, k, λ)-组态，则当 v 是偶数时，$k-\lambda$ 一定是平方数；当 v 是奇数时，下面的 Diophantine 方程

$$x^2=(k-\lambda)y^2+(-1)^{(v-1)/2}\lambda z^2 \tag{3.18}$$

必有 x，y，z 的不全为零的整数解．

证　设 A 是所设 (v, k, λ)-组态的关联矩阵，则 (2.5) 断言

$$AA^T=B=(k-\lambda)I+\lambda J. \tag{3.19}$$

再根据(2.7)和(3.17)可得

$$(\det(A))^2=\det(B)=k^2(k-\lambda)^{v-1}. \tag{3.20}$$

所以 $k^2(k-\lambda)^{v-1}$ 是平方数．如果 v 是偶数，则由此可知 $k-\lambda$ 必为平方数．定理的前半部分得证．

如果 v 是奇数．由 (3.19) 式可知，在有理数域上

$$B\overset{c}{=}I. \tag{3.21}$$

我们先讨论 $v\equiv 1(\bmod 4)$ 的情形．由 (3.11) 和 (3.16) 可得

$$B\overset{c}{=}(k-\lambda)I_{v-1}\dotplus I_1. \tag{3.22}$$

上式也可以用二次型表出：

$$\begin{aligned}(k-\lambda)(x_1^2+x_2^2+\cdots+x_v^2)+\lambda(x_1+x_2+\cdots+x_v)^2\\=(k-\lambda)(y_1^2+y_2^2+\cdots+y_{v-1}^2)+y_v^2.\end{aligned} \tag{3.23}$$

这里

$$x_i=p_{i1}y_1+p_{i2}y_2+\cdots+p_{iv}y_v \qquad (i=1, 2, \cdots, v), \tag{3.24}$$

方阵 $P=[p_{ij}]$ 是非奇异的有理数方阵．在(3.24)式中，如果 $p_{11}\neq$

1，则令 $x_1 = y_1$；如果 $p_{11} = 1$，则令 $x_1 = -y_1$. 因此总有关系式 $x_1^2 = y_1^2$ 和

$$y_1 = e_2y_2 + e_3y_3 + \cdots + e_vy_v, \tag{3.25}$$

其中 $e_2, e_3, \cdots, e_v$ 是有理数. 由(3.24)和(3.25)可得 $x_2 = p_2y_2 + p_3y_3 + \cdots + p_vy_v$，其中 $p_2, p_3, \cdots, p_v$ 是有理数. 同样，如果 $p_2 \neq 1$，则令 $x_2 = y_2$: 如果 $p_2 = 1$，则令 $x_2 = -y_2$. 因此总又有关系式 $x_2^2 = y_2^2$ 和

$$y_2 = f_3y_3 + f_4y_4 + \cdots + f_vy_v, \tag{3.26}$$

其中 $f_3, f_4, \cdots, f_v$ 仍是有理数. 我们可以继续这样做下去，直到得出

$$y_{v-2} = g_{v-1}y_{v-1} + g_vy_v, \tag{3.27}$$

其中 g_{v-1}, g_v 是有理数. 由 (3.24) 和已得的各关系式，我们得到 $x_{v-1} = q_{v-1}y_{v-1} + q_vy_v$，其中 q_{v-1}，q_v 是有理数. 最后，如令 $x_{v-1} = \pm y_{v-1}$，则给出关系式 $x_{v-1}^2 = y_{v-1}^2$ 和 $y_{v-1} = h_vy_v$，其中 h_v 是有理数. 直到现在，我们没有确定 y_v 的值. 现令 y_v 为一非零有理数，则 $y_{v-1}, y_{v-2}, \cdots, y_1$ 可由前面的各个关系式顺次唯一确定，再由(3.24)又可以唯一确定 $x_1, x_2, \cdots, x_v$. 而且 $x_i^2 = y_i^2 (i = 1, 2, \cdots, v-1)$. 我们把这些有理数代入(3.23)后即得

$$(k-\lambda)x_v^2 + \lambda(x_1 + x_2 + \cdots + x_v)^2 = y_v^2, \tag{3.28}$$

这证明了当 $v \equiv 1 \pmod 4$ 时定理成立.

再讨论 $v \equiv 3 \pmod 4$ 的情形. 这时只需把前面所作的论证稍加变动. 由 (3.21)，(3.11) 和 (3.16) 可得

$$B \dotplus I_1 \overset{c}{=} (k-\lambda)I_{v+1}. \tag{3.29}$$

上式可用二次型表出：

$$\begin{aligned}(k-\lambda)(x_1^2 + x_2^2 + \cdots + x_v^2) + \lambda(x_1 + x_2 \\ + \cdots + x_v)^2 + x_{v+1}^2 \\ =(k-\lambda)(y_1^2 + y_2^2 + \cdots + y_{v+1}^2),\end{aligned} \tag{3.30}$$

这里

$$\begin{gathered}x_i = p'_{i1}y_1 + p'_{i2}y_2 + \cdots + p'_{i,v+1}y_{v+1} \\ (i = 1, 2, \cdots, v+1),\end{gathered} \tag{3.31}$$

方阵 $P' = [p'_{ij}]$ 是非奇异的有理数方阵。和前面一样，我们令 $x_1 = \pm y_1$，并得关系式

$$y_1 = c'_2 y_2 + c'_3 y_3 + \cdots + c'_{v+1} y_{v+1}, \qquad (3.32)$$

其中 $c'_2, c'_3, \cdots, c'_{v+1}$ 是有理数. 再令 $x_2 = \pm y_2$，又得关系式

$$y_2 = f'_3 y_3 + f'_4 y_4 + \cdots + f'_{v+1} y_{v+1}, \qquad (3.33)$$

其中 $f'_3, f'_4, \cdots, f'_{v+1}$ 是有理数. 我们继续这样做下去，直到得出

$$y_{v-1} = g'_v y_v + g'_{v+1} y_{v+1}, \qquad (3.34)$$

其中 g'_v, g'_{v+1} 是有理数. 由(3.31) 式和已得各关系式，我们得到 $x_v = q'_v y_v + q'_{v+1} y_{v+1}$，其中 q'_v, q'_{v+1} 是有理数. 最后，如令 $x_v = \pm y_v$，则给出关系式 $y_v = h'_{v+1} y_{v+1}$，这里 h'_{v+1} 是有理数. 令 y_{v+1} 为一非零有理数，则 $y_v, y_{v-1}, \cdots, y_1$ 和 $x_1, x_2, \cdots, x_{v+1}$ 可由前述各关系式唯一确定，而且 $x_i^2 = y_i^2 (i = 1, 2, \cdots, v)$. 我们把这些有理数代入 (3.30) 式后即得

$$\lambda(x_1 + x_2 + \cdots + x_v)^2 + x_{v+1}^2 = (k - \lambda) y_{v+1}^2, \qquad (3.35)$$

而这又证明了当 $v \equiv 3 \pmod 4$ 时定理成立.

设 a 和 m 都是非零整数，而且 a 和 m 互素. 如果同余式 $x^2 \equiv a \pmod m$ 有解，则称 a 是 m 的**二次剩余**；如果 $x^2 \equiv a \pmod m$ 无解，则称 a 是 m 的**二次非剩余**. 设 a, b, c 都是非零整数. 并设它们都是无平方因子的，两两互素，而且符号不全一样. 对满足这些条件的 a, b, c，我们把 Diophantine 方程

$$ax^2 + by^2 + cz^2 = 0 \qquad (3.36)$$

称为 Legendre **方程**. Legendre 的一个经典定理断言，方程(3.36)有 x, y, z 的不全为零的整数解的充分必要条件是 $-bc, -ac, -ab$ 分别是 a, b, c 的二次剩余. 这个定理的必要性很明显. 如设 (3.36) 有 x, y, z 的一个非零整数解，则可不妨假定这 3 个整数没有素公因子. 由此可知，若有素数 $p|a$，则 $p \nmid z$. 因为要是 $p|z$ 的话，则 $p|y$，$p^2|ax^2$，从而 $p|x$，这与假定矛盾. 所以从(3.36)可得出 $(bz^{-1}y)^2 \equiv -bc \pmod a$. 另外两个必要条件可相仿得出. Legendre 定理的本质部分在于指出这些必要条件也是充分的. 这个结论远不是明显的.

不难把方程(3.18)变成 Legendre 方程．分别记 $k-\lambda$ 和 λ 的无平方因子部分为 $(k-\lambda)'$ 和 λ'，并令 $(k-\lambda)'$ 和 λ' 的最大公因子为 d，则方程(3.18)对 x, y, z 有一组非零整数解，当且仅当方程

$$dx^2=\frac{(k-\lambda)'}{d}y^2+(-1)^{\frac{v-1}{2}}\frac{\lambda'}{d}z^2 \tag{3.37}$$

对 x, y, z 有一组非零整数解，而方程 (3.37) 是一个 Legendre 方程．所以，如果 v 是奇数而且存在一个 (v, k, λ)-组态，则下列三个数

$$(-1)^{\frac{v+1}{2}}\frac{\lambda'(k-\lambda)'}{d^2}, (-1)^{\frac{v-1}{2}}\lambda', (k-\lambda)' \tag{3.38}$$

应分别是 d, $(k-\lambda)'/d$, λ'/d 的二次剩余．在很多重要的 (v, k, λ)-组态中，v 是奇数并且 k, λ 互素．所以在这种组态中，$k-\lambda, \lambda$ 互素，从而 $d=1$．对这种组态来说，上述第一个必要条件显然能满足．不难验证第三个必要条件也能满足．因为我们总有等式 $k^2=(k-\lambda)+\lambda v$，它说明 $k-\lambda$ 是 λ 的二次剩余．由此可知 $(k-\lambda)'$ 一定是 λ' 的二次剩余．所以，对于 v 是奇数并且 k, λ 互素的 (v, k, λ)-组态来说，定理 3.1 指出了这种 (v, k, λ)-组态存在的必要条件为 $(-1)^{\frac{v-1}{2}}\lambda'$ 是 $(k-\lambda)'$ 的二次剩余．

我们现在已经作好了证明第七章定理 4.3 的准备．

定理 3.2. 当 $n\equiv 1$ 或 $2 \pmod 4$，而且 n 的无平方因子部分至少有一个素因子 $p\equiv 3 \pmod 4$ 时，n 阶有限射影平面不存在．

证　一个 n 阶有限射影平面是一个参数 $v=n^2+n+1, k=n+1, \lambda=1$ 的 (v, k, λ)-组态．这时 v 是奇数并且 k, λ 互素．$n\equiv 1$ 或 $2 \pmod 4$ 表示 $\frac{v-1}{2}$ 是奇数．因此，如果 n 阶射影平面存在，则 -1 应是 p 的二次剩余．但由初等数论可知，-1 是素数 $p\equiv 3 \pmod 4$ 的二次非剩余．

人们猜想所有阶数 $n\equiv 0 \pmod 4$ 的 Hadamard 矩阵都存在．这里我们不能期望定理 3.1 会进一步指出哪些 Hadamard 组态不

存在．因为 Hadamard 组态的参数 $v=4t-1, k=2t-1, \lambda=t-1$；或 $v=4t-1, k'=2t, \lambda'=t$．对应于这些参数的 Diophantine 方程 (3.18) 是

$$x^2=ty^2-(t-1)z^2 \text{ 或 } x^2=ty^2-tz^2. \tag{3.39}$$

第一个方程有解 $x=y=z=1$；第二个方程有解 $x=0, y=z=1$.

§4. 矩阵方程 $AA^T=B$

我们在这一节研究矩阵方程 $AA^T=B$．在以下的讨论中，A 是 v 阶有理数方阵，A^T 是 A 的转置．v 阶方阵 B 由下式

$$B=(k-\lambda)I+\lambda J \tag{4.1}$$

所定义．在(4.1)中，I 和 J 分别是 v 阶单位方阵和 v 阶元素全是 1 的方阵．我们还假设整数 k 和 λ 满足 $0<\lambda<k<v-1$ 和

$$k-\lambda=k^2-\lambda v. \tag{4.2}$$

我们先证明下述定理．

定理 4.1. 设 A 是有理数方阵，而且 $AA^T=B$，则

$$A^TA=(k-\lambda)I+\frac{\lambda}{k^2}A^TJA. \tag{4.3}$$

证 在 §2 中我们已指出 B 是非异的．我们说 B 的逆由

$$B^{-1}=\frac{1}{k-\lambda}I-\frac{\lambda}{k^2(k-\lambda)}J \tag{4.4}$$

给出．事实上，如将 (4.4) 式乘在 B 的表示式 (4.1) 的右边，利用 (4.2)即得 $BB^{-1}=I$．现设 $AA^T=B$，则 $A(A^TB^{-1})=I$．由于矩阵与它的逆矩阵乘法可交换，故得

$$(A^TB^{-1})A=I. \tag{4.5}$$

将(4.4)式代入(4.5)式，得

$$A^T\left(\frac{1}{k-\lambda}I-\frac{\lambda}{k^2(k-\lambda)}J\right)A=I, \tag{4.6}$$

从而

$$A^TA=(k-\lambda)I+\frac{\lambda}{k^2}A^TJA. \tag{4.7}$$

定理 4.1 有若干有意义的推论．设 A 的第 i 列元素之和为 s_i，第 i 列元素的平方和为 t_i．我们可直接算出

$$A^TJA=[s_is_j]\qquad(i,j=1,2,\cdots,v).\tag{4.8}$$

因此从定理 4.1 可得

$$k^2t_i=\lambda s_i^2+k^2(k-\lambda)\qquad(i=1,2,\cdots,v).\tag{4.9}$$

我们再看一种情况．如果 A 是有理数方阵，$AA^T=B$，而且 $JA=kJ$，则 $A^TA=B$．这同样是定理 4.1 的直接推论．人们对有理数域上的相合关系 $B\overset{c}{=}I$ 进行了广泛的研究，这里我们无法详细叙述这些研究．我们仅仅指出，除掉那些不满足定理 3.1 所述的必要条件的 v,k,λ 的值外，在有理数域上一定有 $B\overset{c}{=}I$．另外，如果在有理数域上有 $B\overset{c}{=}I$，则一定存在满足 $AA^T=A^TA=B$ 的有理数方阵 A．这些问题的本身都是很值得研究的，不过由此并没有揭示任何有关 (v,k,λ)-组态的不存在情况的新结果．

研究整数方阵 A 的矩阵方程 $AA^T=B$ 是很自然的．我们先从简单的讨论开始．设 A 是整数方阵，$AA^T=A^TA=B$，则 A 或 $-A$ 一定是 (v,k,λ)-组态的关联矩阵．因为从 $A^TA=B$ 可得出 $t_i=k$，再从 (4.9) 式又可得出 $s_i^2=k^2$．如果 $t_i=k$ 和 $s_i=k$ 成立，则 A 的第 i 列上的元素一定是 0 或 1；如果 $t_i=k$ 和 $s_i=-k$，则 A 的第 i 列元素是 0 或 -1．B 的每个不在主对角线上的元素都是正整数 λ，所以上述 A 的各列元素的两种可能情况不会同时发生．因此 A 或 $-A$ 一定是 (v,k,λ)-组态的关联矩阵．

设 S 和 S' 是整数元素的 n 阶对称方阵．如果存在一个 n 阶整数方阵 P，使

$$P^TSP=S'\tag{4.10}$$

成立，则称 S **整性代表**了 S'．特别地，如果有 n 阶整数方阵 P，使

$$P^TP=S'\tag{4.11}$$

成立，则单位方阵 I 整性代表了 S'．显然，如果一个 (v,k,λ)-组态存在，则 v 阶单位方阵 I 整性代表了 B．以下我们将证明，对某些 v,k 和 λ 的值来说，上述命题的逆命题也对．不过在一般情况

下，判定一个矩阵是否整性代表了另一个矩阵的问题是一个很深刻的未解决的问题．在这个问题上的进展将大大推进我们对 (v, k, λ)-组态的了解．

若 A 是整数元素的矩阵，而且 $AA^T = B$．如果我们乘 A 的某一列以 -1，则矩阵方程 $AA^T = B$ 依然成立．因此，我们可以选取每列元素之和都非负的 A 来讨论．称满足这种要求的 A 具有**规范化形式**．

定理 4.2. 设 A 是整数元素的矩阵，它具有规范化形式，并满足 $AA^T = B$．如果 k 和 λ 的最大公因子 (k,λ) 是无平方因子的，$k-\lambda$ 是奇数，则 A 是一个 (v, k, λ)-组态的关联矩阵．

证　仍记 A 的第 i 列元素之和为 s_i，第 i 列元素的平方和为 t_i．由假设 A 具有规范化形式可知 $s_i \geq 0$．由方程(4.9)可得

$$\lambda s_i^2 \equiv 0 \pmod{k^2} \qquad (i = 1, 2, \cdots, v). \tag{4.12}$$

由于 (k, λ) 是无平方因子的，故从 (4.12) 和 (4.2) 可知每个 $s_i \equiv 0 \pmod k$．我们记 $s_i = u_i k$，代入(4.9)得

$$t_i = \lambda u_i^2 + (k - \lambda) \qquad (i = 1, 2, \cdots, v). \tag{4.13}$$

如果有某个 $u_i = 0$，则 $s_i = 0$，并由(4.13)式可得 $t_i = k - \lambda$．但是

$$s_i^2 \equiv t_i \equiv k - \lambda \equiv 0 \pmod 2, \tag{4.14}$$

故与 $k-\lambda$ 是奇数的假定矛盾．因此每个 $u_i \neq 0$．但 $JAA^TJ = JBJ$ 蕴涵

$$s_1^2 + s_2^2 + \cdots + s_v^2 = k^2 v, \tag{4.15}$$

从而

$$u_1^2 + u_2^2 + \cdots + u_v^2 = v. \tag{4.16}$$

由于每个 $u_i \neq 0$，故每个 $u_i = 1$，$s_i = k$，$t_i = k$．这表明 A 是一个 (v, k, λ)-组态的关联矩阵．

定理 4.2 中关于 (k, λ) 是无平方因子的假定对很多重要的 (v, k, λ)-组态都能满足．例如，有限射影平面和参数 $v = 4t - 1$，$k = 2t - 1$，$\lambda = t - 1$ 的 Hadamard 组态就都满足 $(k, \lambda) = 1$．与此相反，有相当数量的组态不满足 $k - \lambda$ 是奇数的假定．我们

可以指出,当 $k-\lambda$ 是偶数时,定理4.2不一定成立. 这时从(k,λ)无平方因子仍能得出每个 $s_i\equiv 0(\bmod k)$. 但一般来讲不能得出每个 $u_i\neq 0$.

令H是阶数 $n=2$ 或 $n\equiv 0(\bmod 4)$ 的 Hadamard 矩阵. 并使这个H的第1列全是 $+1$. 作这个H的 $n+1$ 次直和

$$H'=H\dotplus H\dotplus\cdots\dotplus H, \tag{4.17}$$

H' 是 n^2+n 阶方阵. 再令 δ 是 n 个分量的行向量. δ 的第1个分量是1,其余 $n-1$ 个分量都是0. 并记

$$\delta'=(\delta,\delta,\cdots,\delta) \tag{4.18}$$

是由 $n+1$ 个 δ 并列而得的一个 n^2+n 维向量. 在 H' 上添加 δ' 为第1行,再在这个 $(n^2+n+1)\times(n^2+n)$ 矩阵上添加这样一列为第1列,这个列的第1个分量是0,其余分量都是1. 最终得出的矩阵A是一个 n^2+n+1 阶方阵. 不难验证A满足矩阵方程 $AA^T=nI+J$. A 也具有规范化形式,但A不是n阶射影平面的关联矩阵. 我们可以指出,当 $n=2^\alpha$ 时,如上构作的矩阵A和射影平面的关联矩阵都存在. 当 $n=2$ 时,它们可分别如下所示:

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}, \tag{4.19}$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.20}$$

我们再说明，当 $n=10$ 时，满足矩阵方阵 $AA^T=nI+J$ 的 n^2+n+1 阶整数方阵也可作出. 为此，先定义 10 阶方阵

$$H^*=\left[\begin{array}{cc|cccc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\
1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
\hline
1 & 1 & & & & & & & & \\
1 & 1 & & 3I-J & & & & I & & \\
1 & 1 & & & & & & & & \\
1 & 1 & & & & & & & & \\
\hline
1 & -1 & & & & & & & & \\
1 & -1 & & -I & & & & 3I-J & & \\
1 & -1 & & & & & & & & \\
1 & -1 & & & & & & & &
\end{array}\right], \tag{4.21}$$

其中 I 是 4 阶单位方阵，J 是 4 阶元素全是 1 的方阵，则 H^* 是一个 10 阶方阵，不难验证 H^* 满足 $H^*H^{*T}=10I$，在这个方程中，I 是 10 阶单位方阵. 我们可以用这个 H^* 来代替前面的 H，按照同样的构作方法将产生一个 111 阶方阵 A，它满足方程 $AA^T=10I+J$. 但 A 与 10 阶射影平面的关联矩阵相差很远，不大可能从 A 导出射影平面的关联矩阵来. 矩阵方程 $AA^T=nI+J$ 有一大批规范化形式的整数解，这些整数矩阵都不能导出射影平面的关联矩阵. 事实上，我们猜想对参数 $v=n^2+n+1$，$k=n+1$ 和 $\lambda=1$ 的矩阵方程 $AA^T=(k-\lambda)I+\lambda J$，只要 n 是偶数以及在有理数域上 $nI+J\overset{c}{=}I$，就一定有整解.

前面已经提到这样的猜想，即所有阶数 $n\equiv 0(\bmod 4)$ 的 Hadamard 矩阵都存在. 我们现在指出，如果矩阵的整性表示的理论更加完备，则这个猜想可望解决. 事实上，由于 2^a 阶的 Hadamard 矩阵一定存在，而且两个 Hadamard 矩阵的直积仍是 Hadamard 矩阵，所以，如能证明当 t 是奇数时，$4t$ 阶 Hadamard 矩阵都存在，也就能断定所有阶数 $n\equiv 0(\bmod 4)$ 的 Hadamard 矩阵都存在. 但是一个阶数为 $4t\geqslant 8$ 的 Hadamard 矩阵等价于一个参数为 $v=4t-1$，$k=2t-1$ 和 $\lambda=t-1$ 的 Hadamard 组态. 这种组态当 $k-$

$\lambda = t$ 为奇数时正是定理 4.2 所讨论的. 因此所有阶数

$$n \equiv 0 \pmod 4$$

的 Hadamard 矩阵的存在问题可以作为一个矩阵的整表示问题.

§ 5. 极值问题

迄今为止,我们对(v, k, λ)-组态的研究一直集中在存在问题上,即确定能使组态存在的 v, k 和 λ 的值的精确范围. 对每一组 v, k 和 λ 的值,确定不同的 (v, k, λ)-组态的个数的计数问题,要比存在问题困难得多,而且看来不是现在所用的方法所能解决的. 在这方面我们仅指出一个问题: 人们猜想素数阶射影平面是唯一的. 还有一些关于(v, k, λ)-组态的重要问题,它们并不直接涉及上述两类基本问题, 其中有些所讨论的是从组态本身的深刻内在性质演化出来的问题. 例如, 有这样一个尚未解决的问题: 设 A 是 n 阶射影平面的关联矩阵,是否存在两个置换矩阵 P 和 Q,其中 $P \neq I$,使 $PAQ=A$ 成立? 这个问题的肯定回答在几何上有重要意义,它将说明每个射影平面都有非恒等的直射变换 (Collineation). 很多重要问题所论及的是有关满足一定附加要求的特殊组态的存在和分类. 举一个特别有意义的例. 如下所示的 n 阶方阵

$$A = \begin{bmatrix} a_0 & a_1 & a_2 \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_3 \cdots & a_0 \end{bmatrix}. \tag{5.1}$$

称为**循环阵**. 2 阶射影平面的关联矩阵 (4.20) 是一个循环阵. 某些 (v, k, λ)-组态的关联矩阵可经行和列的置换变成循环阵. 这类组态等价于数论中的完备差集, 我们将在下一章研究它. 现在先讨论一些把 (v, k, λ)-组态和本书前面引人的某些概念联系起来的极值问题.

设 v, k 是固定的整数,而且

$$1 \leqslant k \leqslant v. \tag{5.2}$$

又设 $\mathfrak{A}(K,K)$ 是每行和每列正好有 k 个 1 的所有 v 阶 (0，1)-矩阵的类. 在第六章中，我们指出类 $\mathfrak{A}(K,K)$ 中每个矩阵 A 都有 $\mathrm{per}(A)>0$. 但对类 $\mathfrak{A}(K,K)$ 中 A 的 $\mathrm{per}(A)$ 的最小值几乎一无所知. 如果 $\mathfrak{A}(K,K)$ 中包含一个 (v,k,λ)-组态的关联矩阵，稍有一些证据使我们猜想这个矩阵的积和式在 $\mathfrak{A}(K,K)$ 中比较小，或者甚至是最小的. 即使对不大的 v，计算的代价都使得人们不去作这种尝试. 在上述问题中，如果把类 $\mathfrak{A}(K,K)$ 换成双随机矩阵的类，则所论问题就是第五章所说的 van der Waerden 猜想.

对 (v,k,λ)-组态的关联矩阵的积和式我们所知不多，但曾用电子计算机对这类问题进行过广泛的计算. 得知阶数为 2，3，4 的射影平面的相应积和式分别是 24，3852，18534400. 一个方阵的积和式在矩阵的行或列的置换下不变，在转置下也不变. 如果对同一组参数 v，k 和 λ，有两个不同的 (v,k,λ)-组态，它们的关联矩阵分别是 A 和 A'，而且 A 和 A' 不能经行或列的置换以及转置后相等，则我们猜想 $\mathrm{per}(A)\neq\mathrm{per}(A')$，显然它们的行列式的绝对值是相等的.

设 Z 是 2 阶射影平面的关联矩阵 (4,20). 7 阶方阵 Z 具有特性

$$\mathrm{per}(Z)=\det(Z)\text{ 的绝对值 }=24. \tag{5.3}$$

我们现在陈述一个有趣的定理而不加证明，它指出了方阵 Z 在积和式理论中所起的特殊作用.

定理 5.1. 设 A 是类 $\mathfrak{A}(K,K)$ 中的一个循环阵.

如果 $k>3$，则

$$\mathrm{per}(A)>\det(A)\text{ 的绝对值}. \tag{5.4}$$

如果 $k=3$，而且

$$\mathrm{per}(A)=\det(A)\text{的绝对值}, \tag{5.5}$$

则 A 可经行或列的置换变成矩阵 Z 的 e 次直和. 从而 $v=7e$，并且 $\mathrm{per}(A)=24^e$.

在有关行列式的极值问题中也会涉及 (v,k,λ)-组态的关联矩阵.

定理 5.2. 设 Q 是 v 阶(0,1)-矩阵，Q 中一共有 τ 个 1. 用下列二式

$$\tau = kv, \tag{5.6}$$

$$\lambda = \frac{k(k-1)}{v-1} \tag{5.7}$$

来定义 k 和 λ. 并设 $0<\lambda<k<v-1$，则

$$\det(Q)\text{的绝对值} \leqslant k(k-1)^{(v-1)/2}, \tag{5.8}$$

而且(5.8) 中等号成立当且仅当 Q 是一个(v, k, λ)-组态的关联矩阵.

我们在这里不来证明定理 5.2. 实际上这个定理可以在几个方向上推广. 形如(5.8)的不等式看来不大可能解决某些与(v, k, λ)-组态有关的深刻的算术问题. 但这些不等式本身很有意义.注意到定理 5.2 指出，如果在类 $\mathfrak{A}(K, K)$ 中包含一个 (v, k, λ)-组态的关联矩阵的话，则这个关联矩阵的行列式的绝对值在类 $\mathfrak{A}(K, K)$ 中达到最大. 这个事实是比较意外的. 因为我们在前面指出，这个关联矩阵的积和式有可能在类 $\mathfrak{A}(K, K)$ 中最小.

下面我们再指出一个把有限射影平面和第六章所定义的 1-宽度概念联系起来的有意义的结果.

定理 5.3. 设类 $\mathfrak{A}(K, K)$ 的参数 $v = n^2 + n + 1$，$k = n^2$，$n > 2$. 类 $\mathfrak{A}(K, K)$ 中的矩阵如果是 n 阶射影平面的关联矩阵的补，则其 1-宽度 $\varepsilon(1) = 3$. $\mathfrak{A}(K, K)$ 中所有其它矩阵的 1-宽度 $\varepsilon(1) = 2$.

证 证明几乎是直接的. 设 A 是 $\mathfrak{A}(K, K)$ 中的矩阵. 我们作 A^TA. 并分别记 A^TA 中不在主对角线上的元素的最小值和平均值为 λ' 和 λ. 易知

$$\lambda = \frac{n^2(n^2-1)}{n^2+n} = n(n-1). \tag{5.9}$$

如果 $\lambda' = \lambda$，则 A 一定是 n 阶射影平面的关联矩阵的补. 这时等式 $v = n^2 + n + 1$，$k = n^2$ 和 $\lambda = n(n-1)$蕴涵着 A 的每个 $v \times$

2 子矩阵中正好有一行全是 0. 而这表示 A 的 1-宽度 $\varepsilon(1)=3$. 另一方面,如果 $\lambda'<\lambda$, 则等式 $v=n^2+n+1$, $k=n^2$ 蕴涵 $\lambda'=\lambda-1$. 而这将说明在 A 中有某一个 $v\times 2$ 子矩阵,它没有一行全是 0. 所以 A 的 1-宽度 $\varepsilon(1)=2$.

如记定理 5.3 所论的类 $\mathfrak{A}(K, K)$ 中的矩阵的最大 1-宽度为 $\bar{\varepsilon}(1)$, 则定理 5.3 说明, 如果存在 n 阶射影平面, 就有 $\bar{\varepsilon}(1)=3$. 否则 $\bar{\varepsilon}(1)=2$. 在第六章中, 我们分别用 $\tilde{\varepsilon}(\alpha)$ 和 $\bar{\varepsilon}(\alpha)$ 来表示规范类 $\mathfrak{A}(R, S)$ 中矩阵的最小 α-宽度和最大 α-宽度. 我们还指出有一种很有效的方法来计算 $\tilde{\varepsilon}(\alpha)$, 但对 $\bar{\varepsilon}(\alpha)$ 的性质所知很少. 定理 5.3 再次说明了 $\bar{\varepsilon}(\alpha)$ 的极度复杂性.

参 考 文 献

Bose 的[3]是关于 (b, v, r, k, λ)-组态的经典论文. 我们关于 Fisher 不等式的证明取自 Bose 的[4]. 关于 Steiner 三连系可参看[12,17,21,34,36,40,42,52]. 定理 2.1 发表在 Ryser 的[43]中. 8 阶射影平面的唯一性是 Hall, Swift 和 Walker 在[20]中证明的. 关于 Hadamard 矩阵,在[2,6,10,14,38,56,57,58]中都有讨论. 第三节基于 Chowla 和 Ryser 的[8]以及 Bruck 和 Ryser 的[7]. 在 Nagell 的[35]中可以参看对 Legendre 方程的讨论. 第四节大部分是根据 Ryser 的[44], 与此紧密相关的工作可见[1,13, 19, 28]. 第四节的背景材料可参看 Jones 的[29]和 Taussky 的[54]. 在 Nikolai 的[37]中讨论了积和式的计算. 定理 5.1 取自 Tinsley 的[55]; 定理 5.2 发表在 Ryser 的[45,46]中, Marcus 和 Gordon [33] 又讨论了这些结果的推广.

[1] A. A. Albert, Rational normal matrices satisfying the incidence equation, *Proc. Amer. Math. Soc.*, **4** (1953), 554—559.

[2] L. Baumert, S. W. Golomb and M. Hall. Jr., Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.*, **68** (1962), 237—238.

[3] R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugen.*, **9** (1939), 353—399.

[4] ——————, A note on Fisher's inequality for balanced incomplete block designs, *Ann. Math. Stat.*, **20** (1949), 619—620.

[5] R. C. Bose and D. M. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Stat.*, **30** (1959), 21—38.

[6] A. Brauer, On a new class of Hadamard determinants, *Math. Zeit.*, **58** (1953), 219—225.

[7] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canad. Jour. Math.*, **1**(1949), 88—93.

[8] S. Chowla and H. J. Ryser, Combinatorial problems, *Canad. Jour. Math.*,

2 (1950), 93—99.

[9] W. S. Connor, On the structure of balanced incomplete block designs, *Ann. Math. Stat.*, **23** (1952), 57—71.

[10] E. C. Dade and K. Goldberg, The construction of Hadamard matrices, *Michigan Math. Jour.*, **6** (1959), 247—250.

[11] R. A. Fisher and F. Yates, Statistical Tables for Biological Agricultural, and Medical Research, London. Oliver and Boyd, 2nd edition, 1943.

[12] N. K. Fort. Jr., and G. A. Hedlund, Minimal coverings of pairs by triples, *Pacific Jour. Math.*, **8** (1958), 709—719.

[13] J. K. Goldhaber, Integral p-adic normal matrices satisfying the incidence equation, *Canad, Jour. Math.*, **12** (1960), 126—133.

[14] W. Gruner, Einlagerung des Regulären n-Simplex in den n-dimensionalen Würfel, *Comment. Math. Helv.*, **12** (1939—1940), 149—152.

[15] M. Hall, Jr., Some Aspects of Analysis and Probability, New York, Wiley, 1958, 35—104.

[16] ——————, The Theory of Groups, New York. Macmillan, 1959.

[17] ——————, Automorphisms of Steiner triple systems, IBM *Jour. Reserch and Dev.*, **4** (1960), 460—472.

[18] M. Hall, Jr., and W. S. Connor, An embedding theorem for balanced incomplete block designs, *Canad. Jour. Math.*, **6** (1953), 35—41.

[19] M. Hall, Jr., and H. J. Ryser, Normal completions of incidence matrices, *Amer. Jour. Math.*, **76** (1954), 581—589.

[20] M. Hall, Jr., J. D. Swift, and R. J. Walker, Uniqueness of the projective plane of order eight, *Math. Tables Aids Comput.*, **10** (1956), 186—194.

[21] H. Hanani, A note on Steiner triple systems, *Math. Scand.*, **8** (1960), 154—156.

[22] ——————, The existence and construction of balanced incomplete block designs, *Ann. Math. Stat.*, **32** (1961), 361—386.

[23] A. J. Hoffman, M. Newman, E. G. Straus and Taussky, On the number of absolute points of a correlation, *Pacific Jour. Math.*, **6** (1956), 83—96.

[24] A. J. Hoffman and M. Richardson, Block design games, *Canad. Jour. Math.*, **13** (1961), 110—128.

[25] D. R. Hughes, Collineations and generalized incidence matrices, *Trans. Amer. Math. Soc.*, **86** (1957), 284—296.

[26] ——————, Generalized incidence matrices over group algebras, *Illinois Jour. Math.*, **1** (1957), 545—551.

[27] J. R. Isbell, A class of simple games, *Duke Math. Jour.*, **25** (1958), 423—439.

[28] E. C. Johnsen, Matrix rational completions satisfying generalized incidence equations, and integral solutions to the incidence equation for finite projective plane cases of orders $n \equiv 2 \pmod 4$; doctoral dissertation , Ohio state University, 1961.

[29] B. W. Jones, The Arithmetic Theory of Quadratic Forms, Carus Math. Monograph, no. 10, New York. Wiley, 1950.

[30] E. Kleinfeld, Finite Hjelmslev planes, *Illinois Jour. Math.*, **3** (1959),

403—407.

[31] K. N. Majumdar, On some theorems in combinatorics relating to incomplete block designs, *Ann. Math. Stat.*, 24 (1953), 377—389.

[32] H. B. Mann, Analysis and Design of Experiments, New York, Dover, 1949.

[33] M. Marcus and W. R. Gordon, Generalizations of some inequalities of H. J. Ryser, to appear in *Illinois Jour. Math.*

[34] E. H. Moore, Concerning triple systems, *Math. Ann.* **43** (1893), 271—285.

[35] T. Nagell, Introduction to Number Theory, New York, Wiley, 1951.

[36] E. Netto, Lehrbuch der Combinatorik, Leipzig. Teubner, 2nd edition, 1927, reprinted by Chelsea.

[37] P. J. Nikolai, Permanents of incidence matrices, *Math. Comput.*, **14** (1960), 262—266.

[38] R. E. A. C. Paley, On orthogonal matrices, *Jour. Math. and Physics*, 12 (1933), 311—320.

[39] E. T. Parker, On collineations of symmetric designs, *Proc. Amer. Math. Soc.*, **8** (1957), 350—351.

[40] M. Reiss, Über eine Steinersche combinatorische Aufgabe welche im 45sten Bande dieses Journals, Seite 181, gestellt worden ist, *Crelle's Jour.*, **56** (1859), 326—344.

[41] M. Richardson, On finite projective games, *Proc. Amer. Math. Soc.*, **7** (1956), 458—465.

[42] W. W. Rouse Ball, Mathematical Recreations and Essays (revised by H. S. M. Coxeter), New York, Macmillan, 1947.

[43] H. J. Ryser, A note on a combinatorial problem, *Proc. Amer. Math. Soc.*, **1** (1950), 422—424.

[44] ——————, Matrices with integer elements in combinatorial investigations, *Amer. Jour. Math.*, 74 (1952), 769—773.

[45] ——————, Inequalities of compound and induced matrices with applications to combinatorial analysis, *Illinois Jour. Math.*, **2** (1958), 240—253.

[46] ——————, Compound and induced matrices in combinatorial analysis, *Proc. of Symposia in Applied Math.*, **10** (1960), 149—168.

[47] ——————, Matrices of zeros and ones, *Bull. Amer. Math. Soc.*, **66** (1960), 442—464.

[48] M. P. Schützenberger, A non-existence theorem for an infinite family of symmetrical block designs, *Ann. Eugen.*, **14** (1949), 286—287.

[49] S. S. Shrikhande, The impossibility of certain symmetrical balanced incomplete block designs, *Ann. Math. Stat.*, **21** (1950), 106—111.

[50] ——————, The non-existence of certain affine resolvable balanced incomplete block designs, *Canad. Jour. Math.*, **5** (1953), 413—420.

[51] R. Silverman, A metrization for power sets with applications to combinatorial analysis, *Canad. Jour. Math.*, **12** (1960), 158—176.

[52] T. Skolem, Some remarks on the triple systems of Steiner, *Math. Scand.* **6**(1958), 273—280.

[53] D. A. Sprott, Note on balanced incomplete block designs, *Canad. Jour. Math.*, **6** (1954), 341—346.
[54] O. Taussky, Matrices of rational integers, *Bull. Amer. Math. Soc.*, **66** (1960), 327—345.
[55] M. F. Tinsley, Permanents of cyclic matrices, *Pacific Jour. Math.*, **10** (1960), 1067—1082.
[56] J. A. Todd, A combinatorial problem, *Jour. Math. Phys.*, **12** (1933), 321—333.
[57] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. Jour.*, **11** (1944), 65—81.
[58] ————, Note on Hadamard's determinant theorem, *Bull. Amer. Math. Soc.*, **53** (1947), 608—613.

第九章　完备差集

§1. 完备差集

设 $d_1, d_2, \cdots, d_k$ 是模 v 的整数，而且每个 $a \neq 0 \pmod v$ 正好可以用 λ 种方式表为

$$d_i - d_j \equiv a \pmod v. \tag{1.1}$$

我们再假定

$$0 < \lambda < k < v - 1. \tag{1.2}$$

这时，我们称 k-集 $D = \{d_1, d_2, \cdots, d_k\}$ 为一个完备差集，或简称差集．不等式(1.2)只用来排除某些退化情况．不难验证

$$\lambda = \frac{k(k-1)}{v-1}, \tag{1.3}$$

关系式(1.3)也是下述定理的直接推论．

定理1.1. 完备差集D等价于一个其关联矩阵是循环阵的(v, k, λ)-组态．

证　设X是整数 $0, 1, \cdots, v-1 \pmod v$ 的 v-集，D是给定的完备差集．我们定义 v 个差集

$$D_e = \{d_1 + e, d_2 + e, \cdots, d_k + e\}$$
$$(e = 0, 1, \cdots, v-1), \tag{1.4}$$

这里每个 D_e 都是X的 k-子集，而且 $D = D_0$．由差集的定义易知每个交集 $D_e \cap D_f (e \neq f)$ 都是X的 λ-子集．从而子集(1.4)是一个(v, k, λ)-组态．而且，X的子集 $D_0, D_1, \cdots, D_{v-1}$ 的关联矩阵是循环阵．同样不难证明逆命题成立．

显然，按照定理1.1，差集可以当作一种特殊的(v, k, λ)-组态，所以第八章的定理3.1也适用于差集．但一般来讲，一个任意的(v, k, λ)-组态不能产生差集．事实上，对很多 v, k, λ 的值，我们知道(v, k, λ)-组态存在而差集并不存在．有多种构作差集

的有效的方法. $\lambda=1$ 时的差集称为**平面的**. $n=k-\lambda$ 时的平面差集相当于一个 n 阶射影平面,这类射影平面称为**循环的**. 对每个素数 p 和正整数 α, Singer 都构作了 $n=p^\alpha$ 阶的循环射影平面. 人们猜想,每个有限的循环射影平面的阶一定形如 p^α. 当 $n\leqslant 1600$ 时,这个猜想已得到证实. 这里顺便提一下,我们还可以猜想每个有限循环射影平面都是 Desarguesian 的,这个猜想实际上已蕴涵了 $n=p^\alpha$. 这里我们不想进一步讨论有意义的 Desarguesian 平面了. 下表列出了关于开头几个 n 的平面差集.

n	v	平面差集
2	7	$\{0,1,3\}$
3	13	$\{0,1,3,9\}$
2^2	21	$\{0,1,4,14,16\}$
5	31	$\{0,1,3,8,12,18\}$
7	57	$\{0,1,3,13,32,36,43,52\}$
2^3	73	$\{0,1,3,7,15,31,36,54,63\}$
3^2	91	$\{0,1,3,9,27,49,56,61,77,81\}$
11	133	$\{0,1,3,12,20,34,38,81,88,94,104,109\}$.

如果参数 v,k,λ 除满足(1.3)外,还满足

$$3\leqslant k\leqslant 50 \tag{1.5}$$

和

$$k<\frac{v}{2}, \tag{1.6}$$

我们可以对相应的差集的存在与否作一概观. 先说明一下,条件(1.6)无损于讨论的一般性,因为差集的补仍是差集. 满足所有这些要求的 v,k,λ 共有 268 组. 对其中 101 组,第八章的定理 3.1 已排除其存在之可能. 在余下的 167 种情况中,已经证明其中有 109 种情况差集不存在,有 46 种情况差集存在. 所以差集存在与否尚未确定的仅有 12 种情况.

有一系列深刻的定理论述了差集的构作,我们只证明下述初等结果.

定理 1.2. 设 p 是素数, $p\equiv 3\pmod 4$, $p\geqslant 7$, 则 p 的 $k=$

$(p-1)/2$ 个不同的二次剩余 $d_1, d_2, \cdots, d_k \pmod p$ 的集合 D 是一个差集，其参数 $v = p = 4t-1, k = 2t-1, \lambda = t-1$.

证 设 c 是 p 的一个二次剩余.又设 d_i 和 d_j 属于 D 而且 $d_i - d_j \equiv 1 \pmod p$，则 $d_i' \equiv cd_i \pmod p$ 和 $d_j' \equiv cd_j \pmod p$ 也属于 D 而且 $d_i' - d_j' \equiv c \pmod p$. 另一方面，如果 d_i' 和 d_j' 属于 D 而且 $d_i' - d_j' \equiv c \pmod p$，则 $d_i \equiv c^{-1}d_i' \pmod p$ 和 $d_j \equiv c^{-1}d_j' \pmod p$ 属于 D 而且满足 $d_i - d_j \equiv 1 \pmod p$. 所以 D 中形如 $d_i - d_j \equiv 1 \pmod p$ 的关系式的个数和形如 $d_i - d_j \equiv c \pmod p$ 的关系式的个数相同. 而当 $p \equiv 3 \pmod 4$ 时，若 c 遍历 p 的 $\frac{p-1}{2}$ 个模 p 的二次剩余 c，则 $-c$ 遍历 p 的 $\frac{p-1}{2}$ 个模 p 的二次非剩余. 另外，$d_i - d_j \equiv c \pmod p$ 等价于 $d_j - d_i \equiv -c \pmod p$. 由此得证 D 是差集.

定理 1.2 中的差集 D 可以产生一个 Hadamard 组态，这个 Hadamard 组态的关联矩阵 A 是循环阵. 这并不意味着每个与 A 相结合的阶数为 $4t = p+1$ 的 Hadamard 矩阵 H 一定是循环阵. 第八章定理 2.5 所说的那种把 A 加边而得到 H 的方法就破坏了 H 的循环性质. 这里暂时离开主题而简单提一下 Hadamard 矩阵和循环阵的关系. 我们知道，4 阶 Hadamard 矩阵

$$H = \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{1.7}$$

是循环阵. 人们猜想阶数 $n>4$ 的 Hadamard 矩阵不可能是循环阵. 可以证明如果 n 阶 Hadamard 矩阵同时又是循环阵，则 n 一定是平方数：如记元素全是 1 的 n 阶方阵为 J，则由于 H 是 Hadamard 矩阵，故 $HH^T = nI$.[*] 又由于 H 是循环阵，故 $HJ = JH = eJ$，这里 e 是一个整数，所以

$$HH^TJ = e^2J = nJ, \tag{1.8}$$

由此即得 $n = e^2$.

§ 2. 乘子定理

设 X 是 $0, 1, \cdots, v-1 \pmod v$ 组成的 v-集，并设 $D=\{d_1, d_2, \cdots, d_k\}$ 和 $D'=\{d'_1, d'_2, \cdots, d'_k\}$ 是对应于同一组参数 v, k, λ 的两个差集. 设整数 t 满足 $(t, v)=1$，s 是任一整数，则 X 的 k-子集 $E=\{td_1, td_2, \cdots, td_k\}$ 和 $E'=\{d'_1+s, d'_2+s, \cdots, d'_k+s\}$ 都是差集. 我们现在要寻求这样的整数 t 和 s，它们使如上定义的 E 和 E' 成为 X 的相同的 k-子集. 如果有这样的整数 t 和 s，则在作差集的分类时，自然可以定义 D 和 D' 是在同构意义下相同的差集. 应该指出，这种 t 和 s 并不一定存在. 例如，不难验证，当 $v=31$ 时，模 31 的二次剩余所成的差集

$$D=\{1,2,4,5,7,8,9,10,14,16,18,19,20,25,28\} \tag{2.1}$$

和差集

$$D'=\{1,2,3,4,6,8,12,15,16,17,23,24,27,29,30\} \tag{2.2}$$

就不能按上述方法变换成同一个差集. 我们不想在这里研究差集的唯一性. 但是，上述讨论提供了一个关于差集的乘子的想法，现在我们稍微详细地研究一下这个概念.

我们称整数 t 为差集 $D=\{d_1, d_2, \cdots, d_k\}$ 的一个**乘子**，如果有整数 s，使得 $E=\{td_1, td_2, \cdots, td_k\}$ 和 $E'=\{d_1+s, d_2+s, \cdots, d_k+s\}$ 成为 X 的相同的 k-子集. 乘子 t 必须对某一个 i 和 j 满足同余式 $td_i - td_j \equiv 1 \pmod v$，因此每个乘子都满足关系

$$(t, v)=1. \tag{2.3}$$

用前面的术语来说，它说明一个乘子必定建立起一个差集到其自身的同构. 显然，我们总有不足道的乘子 $t=1$. 另外，不难验证，模 v 的所有乘子构成乘法群，这个群称为差集的**乘子群**. M. Hall 引入乘子的概念并用以研究差集，事实上这也确实提供了一种导出差集的存在和不存在定理的有力方法. 遗憾的是这个理论对 (v, k, λ)-组态还没有一种已知的类似.

以下开始对乘子作研究. 先对同余关系作若干一般说明，设 $f(x)$，$g(x)$ 和 $h(x)$ 是整系数多项式，如果有另一个整系数多项式

$k(x)$，它使得等式 $f(x)-g(x)=k(x)h(x)$ 成立，则可记成

$$f(x)\equiv g(x)(\bmod h(x)). \tag{2.4}$$

又如果 a 和 b 是任意整数，m 是正整数，而 a' 和 b' 是使

$$a\equiv a'(\bmod m) \text{ 和 } b\equiv b'(\bmod m)$$

成立的非负整数，则 $a\equiv b(\bmod m)$ 当且仅当 $a'\equiv b'(\bmod m)$，而且同余式

$$a\equiv b(\bmod m) \tag{2.5}$$

等价于多项式同余式

$$x^{a'}\equiv x^{b'}(\bmod x^m-1). \tag{2.6}$$

我们把 (2.6) 式换成

$$x^a\equiv x^b(\bmod x^m-1). \tag{2.7}$$

在(2.7)式中出现"负"指数不致于混淆，因为(2.7)不过是 (2.6) 的另一种写法. 于是(2.5) 对整数 a 和 b 成立当且仅当(2.7) 对整数 a 和 b 成立.

现设 $D=\{d_1,d_2,\cdots,d_k\}$ 是一个参数为 v,k,λ 的差集. 定义

$$\theta(x)\equiv x^{d_1}+x^{d_2}+\cdots+x^{d_k}(\bmod x^v-1). \tag{2.8}$$

由于 D 是差集，所以可得

$$\theta(x)\theta(x^{-1})\equiv k+\lambda x+\lambda x^2+\cdots+\lambda x^{v-1}(\bmod x^v-1). \tag{2.9}$$

因为 (2.9) 式左边展开后将等于一些形如 $x^{d_i-d_j}$ 的项的和，其中 $x^0=1$ 正好出现 k 次，$x, x^2, \cdots, x^{v-1}$ 各正好出现 λ 次. 如记

$$T(x)=1+x+\cdots+x^{v-1}, \tag{2.10}$$

则 (2.9) 式可改写成

$$\theta(x)\theta(x^{-1})\equiv k-\lambda+\lambda T(x)(\bmod x^v-1). \tag{2.11}$$

注意到如果 $\varepsilon\neq 1$ 是某个 v 次单位根，则 $T(\varepsilon)=0$. 从而 (2.11) 式蕴涵

$$k-\lambda=\theta(\varepsilon)\theta(\varepsilon^{-1}). \tag{2.12}$$

这个方程有其本身的意义，而且它也告诉我们，差集可导致与单位根有关的因式分解问题. 现在回到乘子问题. 我们注意到，t 是差集 D 的乘子当且仅当

$$\theta(x^t)\equiv x^s\theta(x)(\bmod x^v-1). \tag{2.13}$$

上式左边的指数是 $td_1, td_2, \cdots, td_k(\bmod v)$，右边的指数是 d_1+

$s, d_2+s, \cdots, d_k+s \pmod v$. 现在我们可以证明下述乘子定理.

定理 2.1. 设 D 是参数为 v, k, λ 的差集. 又设 p 是 $k-\lambda$ 的一个素因子, $p\nmid v$, $p>\lambda$, 则 p 一定是差集 D 的乘子.

证 由于 D 是差集, 故有

$$\theta(x)\theta(x^{-1}) \equiv k-\lambda+\lambda T(x) \pmod{x^v-1}. \tag{2.14}$$

若 $f(x)$ 是任一整系数多项式, 则 $T(x)$ 的定义蕴涵

$$f(x)T(x) \equiv f(1)T(x) \pmod{x^v-1}. \tag{2.15}$$

由假定 $p|k-\lambda$ 和 $p\nmid v$ 和已知的关系 $k-\lambda=k^2-\lambda v$ 可知 $p\nmid k$, 因为否则将有 $p|\lambda v$, $p|\lambda$. 这与 $p>\lambda$ 矛盾. 从而

$$k^{p-1} \equiv 1 \pmod p. \tag{2.16}$$

在 $\theta(x)^p$ 的展开式中, 除去 $x^{pd_1}, x^{pd_2}, \cdots, x^{pd_k}$ 外的所有其他项的系数都能被 p 整除. 现在乘 (2.14) 以 $\theta(x)^{p-1}$ 并应用 (2.15), (2.16), 则最终表示式可写成

$$\theta(x^p)\theta(x^{-1}) \equiv \lambda T(x)+pR(x) \pmod{x^v-1}, \tag{2.17}$$

其中 $R(x)$ 是一个整系数多项式. (2.17) 中的表示式 $\theta(x^p)\theta(x^{-1})$ 作为一个次数小于 v 的多项式具有非负整系数. 由此以及条件 $p>\lambda$ 可知, (2.17) 中的 $R(x)$ 被视为次数小于 v 的多项式时, 诸系数为非负整数. 我们再乘 (2.17) 以 $\theta(x)$ 并应用 (2.14), (2.15), 可得

$$(k-\lambda)\theta(x^p) \equiv pR(x)\theta(x) \pmod{x^v-1}. \tag{2.18}$$

(2.18) 中的表示式 $\theta(x^p)$, $R(x)$ 和 $\theta(x)$ 作为次数小于 v 的多项式都具有非负整系数. 而且 (2.18) 的结构告诉我们 $R(x)$ 不可能有多于 1 个的非零项. 故 $R(x)=ax^s$, 其中 a, s 都是非负整数, 在 (2.18) 中, 如令 $x=1$, 则可得 $k-\lambda=pR(1)$. 从而

$$(k-\lambda)\theta(x^p) \equiv (k-\lambda)x^s\theta(x) \pmod{x^v-1}. \tag{2.19}$$

并可得知 p 一定是乘子.

定理 2.1 建立了每个平面差集的非不足道乘子的存在性, 因为这时定理 2.1 的要求 $p\nmid v$ 和 $p>\lambda$ 肯定满足. 在上述证明中, $p>\lambda$ 的限制条件是关键性的. 但我们猜想这个限制并不是定理的必不可少的假设条件. 另外, 所有已知的差集都有 $(k-\lambda, v)=$

1. 所以人们可以猜想事实上 $k-\lambda$ 的每一个因子都是差集的乘子.

我们不加证明地叙述一个定理，它是上述乘子定理的推广.

定理 2.2. 设 D 是参数为 v, k, λ 的差集. 设 d 是 $k-\lambda$ 的一个因子,而且 $(d, v)=1$, $d>\lambda$. 又设 t 是一个整数，对于 d 的每个素因子 p 都有某个整数 i 使 $p^i \equiv t \pmod v$,则 t 是差集 D 的乘子.

从乘子的概念可以导出若干有意义的定理，我们在这里不去研究这些结果，而仅限于用几个简单的例子来表明怎样利用乘子去建立某些差集的存在性和不存在性,从而结束本章.

例 (a)存在参数 $v=37$, $k=9$, $\lambda=2$ 的差集.设 $D=\{d_1, d_2, \cdots, d_k\}$ 是一个具有参数 v, k, λ 的差集. 如果对 D 的某个乘子 t 成立 $D=\{td_1, td_2, \cdots, td_k\}$，则称 D 对乘子 t 是**不动的**. 假设 $(t-1, v)=1$，则我们可以证明必存在一个 u，使得差集 $D_u=\{d_1+u, d_2+u, \cdots, d_k+u\}$ 对 t 是不动的. 事实上，乘子 t 把差集 D_u 映到差集

$$D_{s+tu}=\{d_1+s+tu, d_2+s+tu, \cdots, d_k+s+tu\} \qquad (2.20)$$

之上,从而当 u 由

$$(t-1)u \equiv -s \pmod v \qquad (2.21)$$

决定时,差集 D_u 对乘子 t 是不动的.现假定有参数 $v=37$,$k=9$, $\lambda=2$ 的差集. 由于 $p=k-\lambda=7$, $7\nmid 37$, $7>2$, 故由定理 2.1 可知 $p=7$ 是此差集的一个乘子. 又由于 $(6,37)=1$, 故存在一个对 7 不动的差集. 我们可以对此差集的各元素同乘某一适当因子,以使差集中有一个元素是 1,则下列 $7 \pmod{37}$ 的各次幂

$$\{1,7,9,10,12,16,26,33,34\} \qquad (2.22)$$

都应是此差集的元素,而事实上 (2.22) 就是一个参数 $v=37$, $k=9$, $\lambda=2$ 的差集. 由上述构作可知，具有这组参数的差集在同构意义下是唯一的.

(b) 存在参数 $v=23$, $k=11$, $\lambda=5$ 的差集. 这时 $k-\lambda=6$, 而且 6 的两个素因子都小于 5,所以不能直接用定理 2.1. 但是我

们有 $9 \equiv 2^5 \pmod{23}$ 和 $9 \equiv 3^2 \pmod{23}$，所以 $t = 9$ 和 $d = 6$ 满足定理 2.2 的要求，故 9 是差集的一个乘子．又由于 $(8,23) = 1$，故存在一个对 9 不动的差集．可以不妨假定 1 是此差集的元素，则下列 $9 \pmod{23}$ 的各次幂

$$\{1,2,3,4,6,8,9,12,13,16,18\} \tag{2.23}$$

都应是此差集的元素．和例(a)一样，(2.23)就是参数 $v = 23, k = 11, \lambda = 5$ 的唯一的差集．易于验证 2 和 3 都是这个差集的乘子．

(c) 不存在参数 $v = 111, k = 11, \lambda = 1$ 的平面差集．这是 10 阶循环射影平面的情况．由定理 2.1 可知 $p = 2$ 是一个乘子．又根据 $(1,111) = 1$，故存在一个对 2 不动的差集．如果我们应用乘子 2 于此差集，则可得

$$\theta(x^2) = \theta(x) \pmod{x^{111} - 1}. \tag{2.24}$$

令 ε 是 3 次单位根，$\varepsilon \neq 1$．由于 $111 = 3 \cdot 37$，故

$$\theta(\varepsilon^2) = \theta(\varepsilon). \tag{2.25}$$

这表示 $\theta(\varepsilon) = \theta(\varepsilon^{-1})$ 是有理数，于是(2.12)式断言 $k - \lambda = 10$ 必为平方数，由此可知 10 阶循环射影平面不存在．

参 考 文 献

关于差集的经典工作有 Singer [12] 和 Hall [4]．这里 §2 的叙述基于 Hall [4] 和 Hall 及 Ryser [6]．定理 2.2 的证明可参看 Hall [5]．

[1] R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.*, **78** (1955), 464—481.

[2] T. A. Evans and H. B. Mann, On simple difference sets, *Sankhyā*, **11** (1951), 357—364.

[3] B. Gordon, W. H. Mills, and L. R. Welch, Some new difference sets, *Canad. Jour. Math.*, **14** (1962), 614—625.

[4] M. Hall. Jr., Cyclic projective planes, *Duke Math. Jour.*, **14** (1947), 1079—1090.

[5] ——————, A survey of difference sets, *Proc. Amer. Math. Soc.*, **7** (1956), 975—986.

[6] M. Hall. Jr., and H. J. Ryser, Cyclic incidence matrices, *Canad. Jour. Math.*, **3** (1951), 495—502.

[7] A. J. Hoffman, Cyclic affine planes, *Canad. Jour. Math.*, **4** (1952), 295—301.

[8] D. R. Hughes, Partial difference sets, *Amer. Jour. Math.*, 78 (1956), 650—674.

[9] E. Lehmer, On residue difference sets, *Canad. Jour. Math.* **5**, (1953), 425—432.
[10] H. B. Mann, Some theorems on difference sets, *Canad. Jour. Math.*, **4** (1952), 222—226.
[11] T. G. Ostrom, Concerning difference sets, *Canad. Jour. Math.*, **5** (1953), 421—424.
[12] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377—385.
[13] R. G. Stanton and D. A. Sprott, A family of difference Sets, *Canad. Jour. Math.*, **10** (1958), 73—77.
[14] R. Turyn and J. Storer, On binary sequences, *Proc. Amer. Math. Soc.*, **12** (1961), 394—399.
[15] A. L. Whiteman, A family of difference sets, *Illinois Jour. Math.*, **6** (1962), 107—121.

记 号 表

$s \in S$ s 是 S 的元素

$A \subseteq S$ A 是 S 的子集

$A \subset S$ A 是 S 的真子集

$P(S)$ S 的所有子集的集

$\varnothing$ 空集

$S \cap T$ S 和 T 的交集

$S \cup T$ S 和 T 的并集

n-集 具有 $n > 0$ 个元素的有限集

$S \times T$ S 和 T 的积集

$(a_1, a_2, \cdots, a_r)$ 有序 r-组，称为大小是 r 的样品，简称 r-样品．如果 r 个分量互不相同，又都从同一 n-集中选出，则称为 n 个元素的一个 r-排列

$P(n,r)$ n 个元素的 r-排列的个数

$n!$ n 阶乘

$G(S)$ S 到自身上的所有 1-1 映射的集

S_n n 级对称群

$\{a_1, a_2, \cdots, a_r\}$ r 个不一定互不相同的元素的无序组，称为大小是 r 的无序选取，简称 r-选取．如果各分量互不相同，则称为 r-子集，如果各分量互不相同，又都从同一个 n-集中选出，则称为 n 个元素的一个 r-组合．

$C(n,r) = \binom{n}{r}$ 二项式系数

$w(a)$ a 的权

$[x]$ $\leqslant x$ 的最大整数

(a,b) a 和 b 的最大正公因数

$a|b$ a 除尽 b

$a\nmid b$ a 除不尽 b

$\varphi(n)$ Euler φ-函数

$\mu(n)$ Möbius 函数

$\pi(x)$ $\leqslant x$ 的素数个数

D_n n 个元素的更列的个数

$A = [a_{ij}]$ 长方阵列：如果元素取自某一域，则称为矩阵

A^T A 的转置

$\operatorname{per}(A)$ A 的积和式

$\det(A)$ A 的行列式

$(0,1)$-矩阵 元素是 0 和 1 的矩阵

I 单位矩阵

J 元素全是 1 的矩阵

U_n 入座数

C 在 $(1,2),(2,3),(3,4),\cdots,(n,1)$ 位置处是 1 在其它位置上都是 0 的 $(0,1)$-矩阵

l_n 第 1 行和第 1 列都是自然顺序的拉丁方的个数

$P_r(S)$ S 的所有 r-子集的集

$N(q_1, q_2, \cdots, q_t, r)$ Ramsey 定理中的最小正整数

N_m 凸 n-边形定理中的最小正整数

SDR 相异代表组

SCR 公共代表组

ρ 项秩

$R = (r_1, r_2, \cdots, r_m)$ 行和向量

$S = (s_1, s_2, \cdots, s_n)$ 列和向量

τ $(0,1)$-矩阵中 1 的个数

$\mathfrak{U} = \mathfrak{U}(R,S)$ 行和向量等于 R，列和向量等于 S 的所有 $(0,1)$-矩阵的类

$\bar{A}$ 极大矩阵

$S \prec S^*$ S 为 S^* 所优超

$\tilde{A}$ 在 $\mathfrak{U}$ 中构作的一个特殊的矩阵

$\tilde{\rho}$ 规范类 $\mathfrak{U}$ 中矩阵的最小项秩

$\bar{\rho}$ 规范类 $\mathfrak{U}$ 中矩阵的最大项秩

$N_0(Q)$ 在 $(0,1)$-矩阵 Q 中 0 的个数

$N_1(Q)$ 在 $(0,1)$-矩阵 Q 中 1 的个数

$\tilde{\sigma}$ 规范类 $\mathfrak{U}$ 中矩阵的最小迹

$\bar{\sigma}$ 规范类 $\mathfrak{U}$ 中矩阵的最大迹

$\varepsilon(\alpha)$ α-宽度

$\tilde{\varepsilon}(\alpha)$ 规范类 $\mathfrak{U}$ 中矩阵的最小 α-宽度

$\bar{\varepsilon}(\alpha)$ 规范类 $\mathfrak{U}$ 中矩阵的最大 α-宽度

$\mathfrak{U}(K,K)$ $R = S = K = (k, k, \cdots, k)$ 的

类

$GF(p^a)$　Galois 域

π　射影平面

B　主对角线元素为 k，其它位置上是 λ 的 v 阶方阵

H　Hadamard 矩阵

$A\times A'$　A 和 A' 的直积

$S^c S'$　S 和 S' 相合

$A \dotplus A'$　A 和 A' 的直和

$D=\{d_1, d_2, \cdots, d_k\}$　完备差集

t　差集的乘子

$\theta(x)$　$x^{d_1}+x^{d_2}+\cdots+x^{d_k}(\bmod x^v-1)$

$T(x)$　$1+x+\cdots+x^{v-1}$

人 名 索 引

（人名后数字指出现的章节．如“8.§5”表示第八章§5，“8.文”表示第八章的参考文献．）

Albert, A. A. 8.文
Bachet. 1.§1
Baumert, L. 8.文
Berge, C. 5.文
Bernoulli. 2.§1
Bose, R. C. 7.§2,7.文,8.文
Brauer, A. 8.文
Bruck, R. H. 7.§4,7.文8.文,9.文
Bussey, W. H. 7.文
Chowla, S. 8.文
Connor, W. S. 8.文
Coxeter, H. S. M. 8.文
Dade, E. C. 8.文
Dickson, L. E. 1.文,2.文
Dulmage, A. L. 5.文,6.文
Eratosthenes. 2.§3
Erdös. 3.§3,3.文
Euler 1,§1,2.§2,3.§1,7.§2
Evans, T. 6.文
Evans, T. A. 9.文
Everett, C. J. 5.文
Ezra, Rabbi Ben 1.§1
Feller, W. 1.文,2.文
Fisher, R. A. 8.§1,8.文
Ford, L.R., Jr. 5.文,6.文
Fort,M. K., Jr 8.文
Fulkerson, D. R. 5.文,6.文
Gale, D. 6.文
Gleason, A. M. 4.文
Goldberg, K. 8.文
Goldhaber, J. K. 8.文
Golomb, S. W. 8.文
Goodman, A. W. 4.文
Gordon, B. 9.文
Gordon, W. R. 8.文
Greenwood, R. E. 4.文
Gruner, W. 8.文
Haber, R. M. 6.文
Hall, M., Jr. 5.文,7.文,8.文,9.§2,
9.文
Hall, P. 5.§1,5.文
Halmos, P. R. 5.文
Hanani, H. 8.文
Hardy, G. H. 2.文
Hedlund, G. A. 8.文
Higgins, P. J. 5.文
Hoffman, A. J. 5.文,8.文,9.文
Hughes, D. R. 8.文,9.文
Isbell, J. R. 8.文
Johnsen, E. C. 8.文
Jones, B. W. 8.文
Kaplansky, I. 3.§2,§3,文
Kleinfeld, E. 8.文
König, D. 5.文
Kuhn, H. W. 5.文
Lagrange. 8.§3
Lehmer, E. 9.文
Lucas. 3.§2
MacNeish, H. F. 7.文
Majumdar, K. N. 8.文
Mann, H. B. 5.文,7.文,8.文,9.文
Marcus, M. 5.文,8.文
Mendelsohn, N. S. 5.文,6.文
Mesner, D. M. 8.文
Mills, W. H. 9.文
Minc, H. 5.文
Moore,E. H. 8.文
Nagell, T. 8.文
Netto, E. 1.文,8.文
Newman, M. 5.文,8.文

Nikolai, P. J 8.文
Ore, O. 5.文
Ostrom, T. G. 9.文
Paley, R. E. A. C. 8.文
Parker, E. T. 7.§2,文
Pickert, G. 7.文
Rado, R. 4.文,5.文
Ramsey, F. P. 4.§1,文
Reiss, M 8.§1,文
Richardson, M. 8.文
Riordan, J. 1.文,2.文,3.§3,文
Rouse Ball 8.文
Ryser, H.J. 5.文,6.文,7.§4,文,8.文,9.文
Sade, A. 3.文
Schützenberger, M. P. 8.文
Shrikhande, S. S. 7.§2,文,8.文
da Silva. 2.§2
Silverman, R. 8.文
Singer, J. 9.§1,文
Skolem, T. 4.文,8.文
Skornyakov, L. A. 7.文
Sprott, D. A. 8.文,9.文
Stauton, R. G. 9.文
Stevens, W. L. 7.文
Storer, J. 9.文
Straus, E. G. 8.文
Swift, J. D. 8.文
Sylvester. 2.§2,8.§3
Szekeres, G. 4.文
Tarry, G. 7.§2,文
Taussky, O. 8.文
Tinsley, M. F. 8.文
Todd, J. A. 8.文
Touchard, J. 3.§2,文
Turyn, R. 9.文
van der Waerden 5.文,6.§5,8.§5
Vaughan, H. E. 5.文
Veblen, O. 7.文
Walker, R. J. 8.文
Welch, L. R. 9.文
Whaples, G. 5.文
Whiteman, A. L. 9.文
Williamson, J. 8.文
Wright, E. M. 2.文
Yamamoto, K. 3.§3,文
Yates, F. 8.文
Yŭ (禹) 1.§1

内 容 索 引

α-宽度 α-width 6.§5

~和有限射影平面 ~and finite projective planes 8.§5

最大~ maximal~ 6.§5,8.§5

最小~ minimal~ 6.§5

Bruck-Ryser 定理 Bruck-Ryser theorem 7.§4

(b,v,r,k,λ)-组态 (b,v,r,k,λ)-configuration 8.§1

~的补 complement of~ 8.§1

~的 Fisher 不等式 Fisher inequality for~ 8.§1

~的关联矩阵 incidence matrix of~ 8.§1

同构的~ isomorphic~ 8.§1

~的必要条件 necessary conditions for~ 8.§1

Desarguesian 平面 Desarguesian plane 9.§1

Fibonacci 数 Fibonacci number 3.§1

Galois 域 Galois field 7.§1

Hadamard 组态 Hadamard configuration 8.§2

Hadamard 不等式 Hadamard inequality 8.§2

Hadamard 矩阵 Hadamard matrix 8.§2

~和整表示 ~and integral representations 8.§4,§5

关于~的猜想 conjecture on~ 8.§2,§3,§5

关于循环~的猜想 conjecture on circulants~ 9.§1

~的直积 direct product of~ 8.§2

规范化的~ normalized ~ 8.§2

Kirkman 三连系 Kirkman triple system 8.§1

Kirkman 的女生问题 Kirkman's schoolgirls problem 1.§1,8.§1

Laplace 展开 Laplace expansion 2.§4

Legendre 方程 Legendre equation 8.§3

Legendre 定理 Legendre theorem 8.§3

Ramsey 定理 Ramsey's theorem 4.§1

Steiner 三连系 Steimer triple system 8.§1

(v,k,λ)-组态 (v,k,λ)-configuration 8.§2

~和整表示 ~and integral representation 8.§4

~和最大行列式 ~and maximal determinant 8.§5

~和积和式 ~ and permanent 8.§5

关于~的猜想 conjecture on~ 8.§3,§5

~的关联矩阵 incidence matrix of~ 8.§2

关于~的不存在定理 nonexistence theorem for~ 8.§3

（中文按汉语拼音排序）

b

本质的 1　essential 1　6.§4

补　complement

　(b,v,r,k,λ)-组态的～　～of (b,v,r,k,λ)-configuration　8.§1

　(0,1)-矩阵的～　～of (0,1)-matrix　8.§1

不变量 1　invariant 1　6.§3

　关于～的定理　theorem on～　6.§3

c

猜想　conjecture

　Euler～　Euler～　7.§2

　van der Waerden～　van der Waerden～　5.§5,6.§5,8.§5

　关于直射的～　～on collineation　8.§5

　关于凸m多边形的～　～on convex m-gon　4.§2

　关于循环平面的～～on cyclic planes　9.§1

　关于积和式互不相等的～　～on distinct permanents　8.§5

　关于有限平面的～　～on finite planes　7.§4,8.§5

　关于 Hadamard 矩阵的～　～on Hadamard matrix　8.§3,§5

　关于 Hadamard 循环阵的～　～on Hadamard circulants　9.§2

　关于整表示的～　～on integral representations　8.§5

　关于最小积和式的～　～on minimal permanents　8.§5

　关于乘子的～　～on multipliers　9.§2

　关于 (v,k,λ)-组态的～　～on (v,k,λ)-configurations　8.§3

d

递推　recurrence　3.§1

　～不等式　～inequality　4.§1

点　point　7.§3

　理想～　ideal～　7.§4

　通常～　ordinary～　7.§4

对换　interchange　6.§3

　～的最小数　minimal number of～　6.§3

　～定理　～theorem　6.§3

对称不平衡区组设计(即 (v, k, λ)-组态)　symmetrical balanced incomplete block design　8.§2

e

二项式系数　binomial coefficient　1.§4
二项式定理　binomial theorem　1.§5
二次型　quadratic form　8.§3
　～的相合　congruence of～　8.§3
　矩阵的～　～of matrix　8.§3
二次剩余　Quadratic residue　8.§3
二次非剩余　Quadratic nonresidue　8.§4

f

非本质的1　Unessential 1　6.§4

g

更列　derangement　2.§3
公共代表组　system of common representatives　5.§2
关联矩阵　incidence matrix　5.§4
　(b,v,r,k,λ)-组态的～　～of (b,v,r,k,λ)-configuration　8.§1
　(v,k,λ)-组态的～　～of (v,k,λ)-configuration　8.§2

h

划分　partition　1.§2
　无序～　unordered～　1.§2
　有序～　ordered～　1.§2
幻方　magic square　1.§1

j

迹　trace　5.§5
　最大～　maximal～　6.§4
　最小～　miminal～　6.§4
集合　set　1.§2
渐近公式　asymptotic formula　3.§3
矩阵　matrix　2.§4
　循环～　circulant～　8.§5
　～的相合　congrence of～　8.§3
　～的直积　direct product of～　8.§2
　～的直和　direct sum of～　8.§3
　双随机～　doubly stochastic～　5.§5

Hadamard～　Hadamard～　8.§2
关联～　incidence～　5.§4
～的整表示　integral representation of～　8.§4
极大～　maximal～　6.§1
正规～　normal～　8.§2
置换～　permutation～　5.§4
(0,1)-～(0,1)-～　2.§4,5.§4,6.§1,8.§3
积和式　permanent　2.§4
关于～的猜想　conjecture on～　5.§5,6.§5,8.§5
关于～的公式　formula for～　2.§4
循环阵的～　～of circulant　8.§5
关联矩阵的～　～ot incidence matrix　8.§5

l

拉丁长方　Latin rectangle　3.§3
关于～的渐近公式　asymptotic formula for～　3.§3
～的扩充　extension of～　5.§3,6.§2
关于～的下界　lower bound for～　5.§3
规范化的～　normalized～　3.§3
～的个数　number of～　3.§3
拉丁方　Latin square　3.§3
～的阶　order of～　3.§3
关于～的未解决的问题　unsolved problem on～　6.§2
类 $\mathfrak{U}(K,K)$　class $\mathfrak{U}(K,K)$　6.§5
～中的循环阵　circulants in～　8.§5
～中的最大积和式　maximal permanent in～　6.§5
～中的最小积和式　minimal permanent in～　6.§5,8.§5
类 $\mathfrak{U}(R,S)$　class $\mathfrak{U}(R,S)$　6.§1
～的存在定理　existence theorem for～　6.§1
关于～的对换定理　interchange theorem for～　6.§3
规范的～　normalized～　6.§3
～中矩阵的个数　number of matrices in～　6.§1

p

品种　varieties　8.§1
平衡不完全区组设计　balanced incomplete block design　8.§1
排列　permutation　1.§3

q

区组　blocks　8.§1
区组设计　blocks design　8.§1
群　group　1.§3

~的陪集　coset of~　5.§2
~作为拉丁方　~as Latin square　3.§3
乘子~　multiplier~　9.§2
权　weight　2.§1

r

入座数　ménage number　3.§2

s

射影平面　projective plane　7.§3
~的对偶原理　duality in~　7.§3
~的衔接关系　incidence relation in~　7.§3
四平方定理　four-square theorem　8.§3

t

同构　isomorphism
(b,v,r,k,λ)-组态的~　~of (b,v,r,k,λ)-configurations　8.§1
差集的~　~of difference sets　9.§2
条　line
矩阵的~　~of matrix　5.§5

w

完备组　complete set　7.§1
关于~的存在定理　existence theorem for~　7.§1
完备差集　perfect difference set　9.§1
~和循环阵　~and circulant　9.§1
~和 Hadamard 组态　~and Hadamard configurations　9.§1
不动的~　fixing of~　9.§2
~的同构　isomorphism of~　9.§2
~的乘子　multiplier of~　9.§2
平面~　planar~　9.§1
问题　problem
舞会~　~of dance　5.§5
Montmort~　~of Montmort　2.§3
女生~　~of schoolgirls　1.§1,8.§1
36 名军官~　~of 36 officers　1.§1,7.§2
入座~　problème des ménages　3.§2

x

相合　congruence

矩阵的～　～of matrices　8.§3
多项式的～　～of polynomials　9.§2
二次型的～　～of quardratic forms　8.§3
向量　vector
行和向量　row sum～　6.§1
列和向量　column sum～　6.§1
项秩　term rank　5.§5
关于～的基本定理　fundamental theorem on～　5.§5
中间～　intermediate～　6.§4
最大～　maximal～　6.§4
最小～　minimal～　6.§4

y

杨辉三角形　1.§5
映射　mapping　1.§3
有限域　finite field　7.§1
有限射影平面　finite projective plane　7.§3
～和完备组　～and complete sets　7.§3
～和1-宽度　～and 1-width　8.§5
循环～　cyclic～　9.§1
关于～的存在定理　existence theorem for～　7.§4
关于～的不存在定理　nonexistence theorem for～　7.§4,8.§3
原理　Principle
对偶～　～of duality　7.§3
逐步淘汰～　～of inclusion and exclusion　2.§1
鸽笼～　pigeon-hole～　4.§1

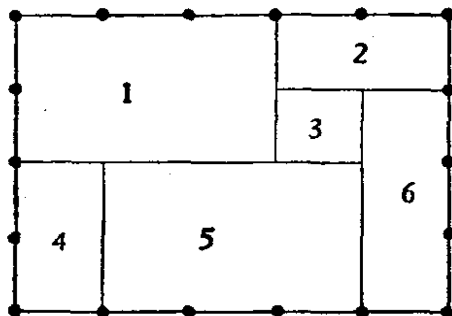
z

阵列　array　2.§4
长方～　rectangular～　2.§4
～的主对角线　main diagonal of～　2.§4
～中的位置　position in～　2.§4
～的型　size of～　2.§4
对称～　symmetric～　2.§4
～的转置　transpose of～　2.§4
正交拉丁方　orthogonal Lartin squares　7.§1
～和有限平面　～and finite planes　7.§4
～的完备组　complete sets of～　7.§1
关于～的 Euler 猜想　Euler conjecture on～　7.§2
～的存在定理　existence theorem for～　7.§1
n≡10(mod 12)阶的～　～for n≡10(mod 12)　7.§2
组合　combination　1.§4

附：组合矩阵论*)

§1. 引论

我们先用一个使人感兴趣的例子来说明怎样用矩阵等式来表述某些组合问题。假定我们有一个矩形 R，它的高和长分别等于正整数 m 和 n. 再把 R 分成 t 个小矩形，每个小矩形的高和长也是正整数. 然后把这些小矩形任意编号为 1，2，…t. 下图是 $m=4$，$n=5$ 和 $t=6$ 的一种情形.



设 A 是一个 m 行 n 列的矩阵，我们就称 A 为 $m\times n$ 型的. 如果 A 的元素只取 0 或 1 这两个整数，则称 A 为一个 (0，1)-矩阵. 现在，我们给上图中的矩形结合上两个分别为 4×6 型和 6×5 型的 (0，1)-矩阵：

$$X=\begin{bmatrix}1&1&0&0&0&0\\1&0&1&0&0&1\\0&0&0&1&1&1\\0&0&0&1&1&1\end{bmatrix},$$

*) 本文是作者根据他于 1973 年 12 月 10—14 日在加利福尼亚大学圣巴巴拉分校举行的矩阵理论会议上所作的讲演写成的. 后来收集发表在《组合学研究》一书的 1—21 页，题为 Combinatorial Matrix Theory. 该书是由 G. C. Rota 主编的一本综述论文集，它是美国数学协会的"数学研究"丛书的第 17 卷，于 1978 年出版. 由于本文完成于作者的《组合数学》一书出版的十年之后，内容又与该书一脉相承且有所补充，所以译出作为它的附录. ——译者注

$$Y = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{1.1}$$

X的第 i 列中所有的 1 一个紧接着一个出现，且 1 的个数等于矩形 i 的高．X的第 i 列中最高的 1 与最低的 1 的位置则标明矩形 i 相对于整个矩形R的上下两条水平边的位置．类似地，Y的第 j 行中所有的 1 也是一个紧接着一个出现，并且 1 的个数等于矩形 j 的长；Y的第 j 行中最左边的 1 与最右边的 1 的位置则标明矩形 j 相对于整个矩形R的左右两条垂直边的位置．如将矩阵X与Y相乘，则得

$$XY = J, \tag{1.2}$$

这里，J是 4×5 型的全 1 矩阵．

这种情况并不是个别的巧合．事实上，由矩阵乘积的定义不难导出，把矩形按上述方式进行划分这件事正好等价于研究矩阵等式(1.2)，其中X和Y分别是 $m\times t$ 和 $t\times n$ 型的 $(0,1)$-矩阵，J是 $m\times n$ 型的全 1 矩阵，并且X的每列中的 1，以及Y的每行中的 1 都是一个紧接着一个出现的．

矩阵理论提供了一种研究种类繁多的组合问题的极有力的工具．以下我们将概述各种各样的课题中的某些课题．由于这整个领域一直是极为活跃的，所以我们既讨论古典结果也讨论近代的结果．

§2. 关联矩阵

设 $X=\{x_1, \cdots, x_n\}$ 是一个 n 元非空集合，我们就说X是一个 n-集．又设 $X_1, \cdots, X_m$ 是 n-集X的 m 个子集，它们不一定互不相同．这个由X及 $X_1, \cdots, X_m$ 构成的组态(configuration)有很大的普遍性，它在组合理论的文献中到处反复出现． 如果当

$x_j \in X_i$ 时令 $a_{ij}=1$，而当 $x_j \notin X_i$ 时令 $a_{ij}=0$，这样得到的 $m\times n$ 型(0, 1)-矩阵

$$A=[a_{ij}] \quad (i=1,\cdots,m;\ j=1,\cdots,n) \tag{2.1}$$

就称为关于 X 的子集 $X_1,\cdots,X_m$ 的**关联矩阵**. A 的第 i 行展示子集 X_i 而第 j 列则展示元素 x_j 是否属于这 m 个子集的情况. 因此，A 给出了子集 $X_1,\cdots,X_m$ 以及元素 $x_1,\cdots,x_n$ 是否属于这些子集的情况的一个完全描述.

我们可以将 n-集 X 的元素以及 X 的这 m 个子集重新标号，这样做并不破坏原有组态的组合内涵. 用关联矩阵的语言来说，重新标号就是用一个新的关联矩阵

$$PAQ \tag{2.2}$$

来代替原来的关联矩阵 A，这里 P 是一个 m 阶置换方阵，Q 是一个 n 阶置换方阵. 所以，我们主要关心关联矩阵在行以及列的任意置换下保持不变的性质.

把一个 n-集的 m 个子集用 $m\times n$ 型的(0,1)-矩阵 A 来表示，这是极为重要的. 因为这使我们能够把强有力的矩阵论技巧用来研究组态的组合性质. 我们总是可以组成矩阵等式

$$AA^T=B \tag{2.3}$$

和

$$A^TA=C, \tag{2.4}$$

这里 A^T 是 A 的转置矩阵. 这时，B 和 C 分别是 m 阶和 n 阶的元素为非负整数的对称方阵. 这些矩阵已经展现了这些子集的不少内在结构. 我们注意到，B 的 (i,j) 元素记录了 $X_i\cap X_j$ 的元素个数，而 C 的 (i,j) 元素则记录了在 m 个子集 $X_1,\cdots,X_m$ 中有多少个同时含有 x_i 和 x_j.

关于(0,1)-矩阵的最著名的一般定理之一是下述的 Kōnig 定理. (这个定理也常称为 Kōnig-Egerváry 定理和 Frobenius-Kōnig 定理.)围绕这个定理以及和它有关的一些定理，如 P. Hall[18] 的关于相异代表元组的定理，Dilworth[10] 的关于偏序集的定理，以及 Ford 和 Fulkerson[12] 的关于极大流与极小截的定理等，有很多文

献．这些论题在 Mirsky 的 [29] 中都有相当详尽的讨论．在[33]中有 König 定理的一个简短而自足的证明．在以下的讨论中，我们把矩阵的一行或一列统称为矩阵的一条．

定理 2.1. 设A是一个$m \times n$型的(0,1)-矩阵．那么，A的可以盖住A中全部 1 的最少的条数等于A中两两不在同一条上的 1 的最大可能个数．

König 定理有如下的集合论解释：从我们的组态中删去一些子集和元素使剩下的子集都是空集时，所必须删去的子集数与元素数之和的最小值等于从每个子集中至多选一个元素时所能选出的两两不同的元素个数的最大值．

§3. 积和式

以$A=[a_{ij}]$表示一个$m \times n$型矩阵，它的元素属于域F，并且设$m \leqslant n$．A的m个两两不在同一条边上的元素之积称为A的一个**对角线积**，A的积和式 per(A) 定义为A的所有对角线积之和，即

$$\operatorname{per}(A)=\sum a_{1i_1}a_{2i_2}\cdots a_{mi_m}, \tag{3.1}$$

这里和式遍取 $1,2,\cdots,n$ 的所有 m-排列 $(i_1,i_2,\cdots,i_m)$．

矩阵A的这个数值函数在组合论文献中到处反复出现．它之所以如此常见的原因之一在于，当A是(0,1)-矩阵时，per(A)等于A的非零对角线积的个数．为了了解积和式，可看文献 [27]*)，那里有积和式的一个详尽的综述．

我们现在讨论n阶方阵的情形，这时，积和式与行列式有着同样类型的表达式，所不同的是，(3.1) 式右边的每个乘积没有 ±1 这样的因子．但是，per(A) 不是A的乘性函数．而且，将A的某一行乘以某一因子再加到另一行上去之后，per(A) 并非不变．这些事实使得求 per(A) 的值比求 det(A) 要困难得多．下述

*) 现在已有更全面的专著[44]．——译者注

关于 per(A) 的公式是逐步淘汰原理[31]的一个推论．我们把矩阵某一行(一条)元素之和称为矩阵的一个行和(条和)．

定理 3.1. 设 A 是元素属于域 F 的一个 n 阶方阵．将 A 的某 r 个列的元素都改为 0 后所得的方阵记为 A_r，A_r 的各行的行和之积记为 $S(A_r)$．我们有

$$\operatorname{per}(A) = S(A) - \sum S(A_1) + \sum S(A_2) - \cdots + (-1)^{n-1}\sum S(A_{n-1}), \tag{3.2}$$

这里和式 $\sum S(A_r)$ 是对所有可能的 A_r 求和．

Jurkat 和 Ryser[21] 引进了求 n 阶方阵 A 的积和式的与此很不相同的技巧．这时把 per(A) 当作 1 阶方阵，并将它表为 n 个矩阵之积，其中每个矩阵都由 A 的单个的行按某种有趣的递推结构组成．对 det(A) 也有类似的矩阵因子分解．我们用 2 阶和 3 阶的情况来说明这种矩阵因子分解等式：

$$[a_1\ a_2]\begin{bmatrix} b_2 \\ \pm b_1\end{bmatrix} = a_1b_2 \pm a_2b_1 = \begin{cases}\operatorname{per}(A)\\ \det(A),\end{cases} \quad A = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2\end{bmatrix},$$

$$[a_1\ a_2\ a_3]\begin{bmatrix} b_2 & b_3 & 0 \\ \pm b_1 & 0 & b_3 \\ 0 & \pm b_1 & \pm b_2\end{bmatrix}\begin{bmatrix} c_3 \\ \pm c_2 \\ c_1\end{bmatrix} = \begin{cases}\operatorname{per}(A)\\ \det(A)\end{cases},$$

$$A = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3\end{bmatrix}.$$

我们指出，将求 per(A) 的两种公式的计算有效性加以比较，这本身就是一个有一定意义的课题[23]．

per(A) 和 det(A) 的矩阵因子分解式提示我们，有可能存在多种多样的富于组合意义的矩阵恒等式．在这方面，我们要指出 Amitsur 和 Levitzki[1] 的一个很值得注意的恒等式．设 $A_1, \cdots, A_k$ 是元素属于域 F 的 n 阶方阵，定义

$$[A_1, \cdots, A_k] = \sum \operatorname{sgn}(\sigma) A_{\sigma 1}\cdots A_{\sigma k}, \tag{3.3}$$

这里和式遍取整数 $1, \cdots, k$ 的所有排列 σ．

定理 3.2. 设 $A_1, \cdots, A_{2n}$ 是元素属于域 F 的 n 阶方阵，则有

$$[A_1, \cdots, A_{2n}] = 0. \tag{3.4}$$

Swan[40,41] 给出了 Amitsur-Levitzki 恒等式的一个基于图论的证明. Amitsur-Levitzki 恒等式是所谓"行列式"类型的. 如能得到"积和式"类型的有关的矩阵恒等式，那将是非常有意义的工作.

积和式理论中最著名的论题是所谓 van der Waerden 猜想. 一个 n 阶方阵称为是双随机阵，即 A 的元素都是非负实数，并且每一个条和都等于 1. van der Waerden 猜想断言，每个 n 阶双随机阵 A 必满足

$$\mathrm{per}(A) \geqslant n!/n^n. \tag{3.5}$$

当 $A = n^{-1}J$(J 是 n 阶全 1 方阵)时，(3.5)式中的等式成立. 这可能是(3.5)式中等式成立的仅有情形. van der Waerden 猜想的正确性只对 n 的头几个很少的值被验证过.

下述 Marcus 和 Newman[28] 的优美的定理，对 van der Waerden 猜想的可能的正确性增加了一些支持: *)

定理 3.3. 设 A 是 n 阶对称半定正的双随机阵，则 A 满足

$$\mathrm{per}(A) \geqslant \frac{n!}{n^n}, \tag{3.6}$$

并且(3.6)式中当且仅当 $A = n^{-1}J$ 时，等号成立.

在研究(0,1)-矩阵的积和式时，还产生了一些有意思的不等式和猜想. 设 A 是 n 阶 (0, 1)-矩阵，A 的每一个条和都等于 k，k 是在区间 $1 \leqslant k \leqslant n$ 内的一个固定的正整数，则 M. Hall[16] 的不等式断言

$$\mathrm{per}(A) \geqslant k!. \tag{3.7}$$

但作为 k 的函数的 per(A) 的最小值还远未为人所知. 事实上，我们可以把定出 per(A) 的这个最小值当作 van der Waerden 原来的问题的"离散形式".

---

*) 有关积和式的更详尽论述，可参看专著 [44] 以及对它的长篇书评; van der Waerden 猜想，近年已得到证实，读者可参看《数学译林》1981 年第 3 期 60—65 页和1982年第 4 期360—365页. ——译者注

§4. 对称区组设计

我们现在来定义一些组态，它们在组合矩阵论中起着很重要的作用，一个 v-集 $X=\{x_1,\cdots,x_v\}$ 的 v 个子集 $X_1,\cdots,X_v$ 称为一个 (v,k,λ)-设计(对称区组设计)，即它们满足下列条件:

$$\text{每个 } X_i \text{ 都是} X \text{的 } k\text{-子集}. \tag{4.1}$$

$$\text{每个 } X_i\cap X_j(i\neq j) \text{都是} X \text{的 } \lambda\text{-子集}. \tag{4.2}$$

$$\text{整数 } v,k,\lambda \text{ 合于 } 0<\lambda<k<v-1. \tag{4.3}$$

由上列条件可知，一个 (v,k,λ)-设计的关联矩阵 A 是一个满足矩阵等式

$$AA^T=(k-\lambda)I+\lambda J \tag{4.4}$$

的 v 阶(0,1)-矩阵. 在(4.4)中，A^T 是矩阵 A 的转置，I 是 v 阶单位阵而 J 是 v 阶全 1 矩阵.

现在我们来证明，(v,k,λ)-设计的关联矩阵 A 必定是正规的，即有

$$AA^T=A^TA. \tag{4.5}$$

由简单的计算可知

$$\det((k-\lambda)I+\lambda J)=(k-\lambda+\lambda v)(k-\lambda)^{v-1}\neq 0. \tag{4.6}$$

从而 A 是非退化矩阵，我们记 A 的逆阵为 A^{-1}，于是，我们有

$$AJ=kJ,\quad A^{-1}J=k^{-1}J. \tag{4.7}$$

(4.4)式两边右乘以 J，得

$$AA^TJ=(k-\lambda+\lambda v)J. \tag{4.8}$$

于是由(4.7)，(4.8)可得

$$A^TJ=(k-\lambda+\lambda v)k^{-1}J. \tag{4.9}$$

再将(4.9)式两边取转置，得

$$JA=(k-\lambda+\lambda v)k^{-1}J. \tag{4.10}$$

从而有

$$JAJ=(k-\lambda+\lambda v)k^{-1}vJ. \tag{4.11}$$

但由(4.7)又可得

$$JAJ=kvJ, \tag{4.12}$$

由此我们就得到有意义的关系式

$$k - \lambda = k^2 - \lambda v. \tag{4.13}$$

于是由(4.13),(4.10)式可得

$$JA = kJ. \tag{4.14}$$

最后,我们有

$$\begin{aligned} A^T A = A^{-1}(AA^T)A &= (k - \lambda)I + \lambda A^{-1}JA \\ &= (k - \lambda)I + \lambda J, \end{aligned} \tag{4.15}$$

而这就是所要的结论.

组合理论的一个主要未解决的问题是确定 v, k, λ 的精确的取值范围,对于在此范围内的参数(v, k, λ)-设计存在. 已经知道参数 v, k, λ 远不是可以任取的,因为它们不仅必须满足(4.3)式,还要合于(4.13)式,此外,所仅知的关于参数的必要条件,即下述 Bruck-Ryser-Chowla 关于 (v, k, λ)-设计的存在定理:

定理 4.1. 假设对整数 v, k 和 λ,存在 (v, k, λ)-设计,那么,如果 v 是偶数,则 $k - \lambda$ 是平方数;如果 v 是奇数,则 x, y, z 的不定方程

$$x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2 \tag{4.16}$$

必有一组不全为零的整数解.

v 是偶数时的断言,可以从(4.6)式中算出的行列式必须等于平方数这一事实直接得知. 但 v 是奇数的情形,就需要对有理数域上的矩阵相合关系作较深入的分析.

参数 v, k 和 λ 的某些特殊集合本身具有很大的重要性. 所谓 n 阶**有限射影平面**就是在参数

$$v = n^2 + n + 1,\ k = n + 1,\ \lambda = 1 \qquad (n \geqslant 2) \tag{4.17}$$

时的 (v, k, λ)-设计. 几何中的有限射影平面相当于代数中的有限域. 但是,所有有限域都已完全弄清楚了,而有限射影平面的结构则远非如此.

当平面的阶数是素数幂时,有限射影平面容易由有限域构作. 有人猜测有限射影平面的阶一定是素数幂. 最小的未定阶数是 $n = 10$. 构作一个 10 阶平面等价于找出一个 111 阶的 (0, 1)-矩阵 A,使得 AA^T 的主对角线上的元素都等于 11,其余元素都是 1.

这个问题已被深入地研究过[26]，并且也许是具有纯有限特点的未解决问题中最著名的一个.

我们现在再指出某些会导致另一类重要的 (v, k, λ)-设计的矩阵. 设H是元素为 1 或 -1 的 n 阶矩阵. 如果H满足矩阵等式

$$HH^T = nI, \tag{4.18}$$

其中 H^T 是H的转置矩阵而 I 是 n 阶单位阵,则称H是 n 阶 Hadamard 矩阵. 不难验证 Hadamard 矩阵的阶是 $n = 1, 2$ 或

$$n \equiv 0 (\mathrm{mod}\ 4).$$

人们猜测,对于一切阶数 $n \equiv 0 (\mathrm{mod}\ 4)$ 一定存在 Hadamard 矩阵. 如今,对于 n 的许多值, n 阶 Hadamard 矩阵已被构造出来了.

一个 Hadamard 矩阵的一行或一列乘以 -1 后仍是 Hadamard 矩阵. 因此我们不妨假定 Hadamard 矩阵的第 1 行和第 1 列的元素都是 1,这样的 Hadamard 矩阵称为规范化的. 现设H是一个规范化的 Hadamard 矩阵,H的阶 $n = 4t \geqslant 8$, 去掉H的第 1 行、第 1 列,再把H中的每个 -1 都改为 0,我们就得到一个 $v = 4t - 1$ 阶的 $(0,1)$-矩阵 A. 从A的结构直接可知, 一个规范化的 $n = 4t \geqslant 8$ 阶 Hadamard 矩阵等价于一个参数为

$$v = 4t - 1, k = 2t - 1, \lambda = t - 1 \qquad (t \geqslant 2) \tag{4.19}$$

的 (v, k, λ)-设计. 这种设计称为 Hadamard 设计. 因此, 关于 Hadamard 矩阵存在性的主要猜想等价于对于一切参数组(4.19)存在 Hadamard 设计的猜想.

再一类近来颇受人注意的特殊的 (v, k, λ)-设计是参数 $\lambda = 2$ 的设计. 这类设计称为双平面,它们实际上很少[8]. 这种设计目前只知道很少几个. 人们实际上是这样猜想的: 对每个固定的值 $\lambda > 1$,(v, k, λ)-设计的个数都是有限的.

我们不想再进一步概述有关对称区组设计的众多文献了, 在 Dembowski[9], Hall [17] 和 Ryser [31]书中都有这种概述.

§ 5. 对称区组设计的近期变体

在 (v, k, λ)-设计的定义中,条件(4.3)并不重要,因为它只用

来排除一些退化情形．但对定义这种组态来说，条件(4.2)却是根本性的．条件(4.1)的状况不大明朗．在 Ryser[32] 和 Woodall[43] 所证明的下述定理中，(4.4) 式右端的数量矩阵被换为一个对角矩阵，从而使我们知道一些当放弃条件(4.1)后将会发生的情况．

定理 5.1. 设 A 是一个 $n\ (>1)$ 阶的(0,1)-矩阵，它满足矩阵等式

$$AA^T = \mathrm{diag}[k_1 - \lambda, \cdots, k_n - \lambda] + \lambda J, \tag{5.1}$$

其中 A^T 是 A 的转置而 J 是 n 阶全 1 阵．假定所有的 k_i 不全相等，而且 $0 < \lambda < k_i (i = 1, \cdots, n)$，则 A 恰有 2 个不同的行和 c_1 及 c_2，这两个数满足

$$c_1 + c_2 = n + 1. \tag{5.2}$$

以定理 5.1 中的矩阵 A 作为关联矩阵的组态，是对称区组设计的变体，称为关于 n 个元素的 λ-设计．$\lambda = 1$ 时的 λ-设计具有特别简单的结构．可以证明，对每个 $n > 3$，$\lambda = 1$ 的 λ-设计唯一存在[7]：

$$X_1 = \{2, 3, \cdots, n\},$$
$$X_2 = \{1, 2\}, X_3 = \{1, 3\}, \cdots, X_n = \{1, n\}.$$

这与有限射影平面的情况截然相反．还可以证明，$\lambda = 2$ 的 λ-设计也唯一存在[32]：

$$\{1,2,4\},\{1,4,6,7\},\{2,5,7,1\},\{3,6,1,2\},\{4,7,2,3\},$$
$$\{5,1,3,4\},\{6,2,4,5\}.$$

通过将对称区组设计的关联矩阵作简单而适宜的变动，我们就可以构造出 λ-设计[2,43]．用这种手续所构造的一切 λ-设计（包括 $\lambda = 1$ 时的 λ-设计)都称为第一类 λ-设计．人们猜想，所有 λ-设计都是第一类的．当 $\lambda \leqslant 9$ 时，这个猜想已被验证为对的[2,4,25]．

我们由此看到，条件(4.1)在对称区组设计中的作用并没有完全弄清楚．人们还不知道当去掉这个条件后是否会有异样的新组态存在．

下述 Woodall 的定理[43]，对于 λ-设计解决了我们原先对 (v, k, λ)-设计提出的那个问题：

定理 5.2. 对每个确定的值 $\lambda > 1$,λ-设计的个数是有限的.

λ-设计可以看成是通过改动矩阵等式 (4.4) 的右端而得到的对称区组设计的一个变体. Bridges 和 Ryser[5] 的下述定理就说到了矩阵等式(4.4)左端的一种改动法:

定理 5.3. 设 X 和 Y 是 $n > 1$ 阶的非负整矩阵,它们合于

$$XY = (k - \lambda)I + \lambda J, \tag{5.3}$$

其中 I 是 n 阶单位阵, J 是 n 阶全 1 阵. 假定 $k \neq \lambda$, 而且整数 k 与 λ 互素,那么, 存在正整数 r 和 s, 使得 X 的每一个条和都等于 r, 而 Y 的每一个条和都等于 s. 这里

$$rs = k + (n - 1)\lambda. \tag{5.4}$$

此外还有

$$XY = YX. \tag{5.5}$$

我们指出,矩阵等式(5.3)本身具有集合论解释,而且 (5.3) 的某些特解导致所谓的强正则图[13,39].

应该注明, 在定理 5.3 中, $k \neq \lambda$ 这个假定是假设条件中的实质部分. 举例说,如将第一节中的矩形 R 取为边长是 n 的正方形. 再将 R 分成 n 个小矩形, 每个小矩形都有整数的高和长. 根据第一节的讨论,这种分割将产生两个 n 阶(0,1)-矩阵 X 和 Y,使得

$$XY = J. \tag{5.6}$$

但这时 X(以及 Y)都未必具有相同的条和.

我们现在设 A 是一个 n 阶(0,1)-矩阵并假定 A 满足矩阵等式

$$A^2 = J. \tag{5.7}$$

这个等式是在研究中心群胚 (central groupoid)、泛代数 (universal algebra) 以及每一对顶点恰好有一条长为 2 的路相连接的图时自然引出的[24]. 这里不去追索它的这些应用. 重要的是要牢记我们所讨论的各种矩阵等式都具有深远的含义.

我们现在来探究满足矩阵等式(5.7) 的 n 阶 (0, 1)-矩阵 A 的结构. 分别用 A 乘(5.7)式的两边,得

$$JA = AJ = A^3. \tag{5.8}$$

然后用 J 左乘 (5.8) 式得

$$J^2A = nJA = JAJ = eJ, \tag{5.9}$$

这里 e 是 A 的所有元素之和．由此可知，A 的每个条和都等于

$$c = \frac{e}{n}. \tag{5.10}$$

但以 J 左乘（或右乘）(5.7)式后又有

$$c^2 = n. \tag{5.11}$$

从而可知满足(5.7)式的 n 阶(0，1)-矩阵 A 的阶数 n 必为平方数．

当 n 是一个平方数时，不难构作(5.7)式的一个"自然"解．例如，对于 $n = 4$，这个"自然"解是：

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

于是人们试图对(5.7)式的所有解作分类．这个问题是 Hoffman[19] 提出的，但至今还没有得到解决．

我们来对满足 (5.7) 式的 (0,1)-矩阵 A 作进一步的计算．矩阵 J 有一个 1 重特征根 n 和一个 $(n-1)$ 重特征根 0，从而由特征根的熟知性质可知，A 具有一个 1 重特征根 $\pm c$ 和一个 $(n-1)$ 重特征根 0．但 A 的 n 个特征根之和应等于 A 的主对角线上元素之和，所以 A 的非零特征根必定是 c 而不是 $-c$。我们的结论是：任一满足方程(5.7)的 n 阶(0，1)-矩阵 A，其主对角线上恰好有 c 个 1。

有人研究过矩阵等式(5.7)的种种推广和变形．对此我们提出下列参考文献：[3,20,34]．

§6. 未定元和关联矩阵*)

我们回到第二节开始所讨论的 n-集 $X = \{x_1, \cdots, x_n\}$ 及其 m 个子集 $X_1, \cdots, X_m$．可以重提一下：X 的这些子集的关联矩

*) 本节可参看 Ryser 后来发表的综述文章[45]．——译者注

阵是一个 $m\times n$ 型的 (0, 1)-矩阵 A，A 的第 i 行展示子集 X_i，而 A 的第 j 列则展示元素 x_j 是否属于这些子集的情况.

现在我们把 n-集 $X=\{x_1, \cdots, x_n\}$ 的元素当作有理数域上的 n 个独立的未定元，并且也用 X 来记 n 阶对角阵

$$X=\mathrm{diag}[x_1, \cdots, x_n]. \tag{6.1}$$

在较近的论文[35]中，Ryser 引入了矩阵等式

$$AXA^T=Y, \tag{6.2}$$

其中 A^T 表示矩阵 A 的转置.

矩阵等式 (6.2) 以一种非常紧凑的方式包含了大量信息. 这里 Y 是一个 m 阶对称方阵而这个方阵的结构我们是清楚的. Y 的 (i,j) 位置上的元素等于 $X_i\cap X_j$ 中的未定元之和. 所以 Y 给出了 n-集 X 的子集 $X_1, \cdots, X_m$ 的所有交集 $X_i\cap X_j$ 的明晰表示.

矩阵等式 (6.2)在讨论某些类型的集合相交问题时是有用的. 也有人研究过一个更广一些的矩阵等式的代数性质[37]. 有关矩阵及集合相交的早期研究有[14,15,22,36]*).

我们现在指出矩阵等式 (6.2) 的一些初等性质. 由关于矩阵的秩的标准的定理可知有

$$\mathrm{rank}(Y)=\mathrm{rank}(A). \tag{6.3}$$

而对于 $m=n$ 这个特殊情形，我们对(6.2)两端取行列式可得

$$\det(Y)=(\det(A))^2\prod_{i=1}^{n}x_i. \tag{6.4}$$

矩阵等式 (6.2) 含有未定元而且我们可赋予这些未定元以任意有理数值. 每赋予一组值就给出描述我们的子集的组态的关联矩阵 A 所必须满足的一个矩阵等式. 例如，令 $x_1=\cdots=x_n=1$，则(6.2)式就变成了先前的等式(2.3)，而 (2.3) 式的矩阵 B 揭示了子集的交中的元素个数. 不能排除矩阵等式 (6.2) 有重要应用的可能性. 这种应用或许是巧妙地赋予未定元以数值，从而使第四、五节的那些未解决问题得到新的启示.

---

*) 还可参看 H. J. Ryser 的最新综述论文[46]. ——译者注

我们现在讨论未定元在组合矩阵论中的一种颇为不同的用法．第二节所说的 Kōnig 定理所处理的是 $m \times n$ 型 (0, 1)-矩阵．这个定理可以直接推广到元素属于域 F 的任意的 $m \times n$ 型矩阵 A.

定理 6.1. 设 A 是元素属于域 F 的 $m \times n$ 型矩阵．那么，A 的可以盖住 A 中全部非零元素的最少条数，等于 A 的两两不在同一条上的非零元素的最大可能个数．

A 中两两不在同一个条上的非零元素个数的最大值，称为 A 的项秩．现在我们放弃早先的记号而以

$$X = [x_{ij}](i = 1, \cdots, m; j = 1, \cdots, n) \tag{6.5}$$

表示一个 $m \times n$ 型矩阵，其元素 x_{ij} 是 F 上 mn 个独立的未定元．我们把 A 与 X 的 Hadamard 积

$$M = A * X = [a_{ij}x_{ij}] \tag{6.6}$$

称为与 A 相伴的形式关联矩阵．M 的元素属于多项式环

$$F^* = F[x_{11}, x_{12}, \cdots, x_{mn}]. \tag{6.7}$$

现在已经知道形式关联矩阵在不少种组合研究中很有用[6,11,30,38,42]．其原因之一在于 A 的一个重要的组合不变量等于 M 的一个代数不变量，即 A 的项秩等于 M 的秩．这个被 Edmonds[11] 所注意到的事实可以这样来推导：由形式关联矩阵的定义可知，M 的一个 r 阶子矩阵的行列式不为零，当且仅当 A 的相应子矩阵的项秩为 r．但矩阵的秩等于具有非零行列式的子方阵的最大阶数，从而可得断言．所以，作为特例，我们有：对于 $m \leqslant n$ 时的一个 $m \times n$ 型的(0,1)-矩阵 A，$\mathrm{per}(A) > 0$，当且仅当 M 的秩是 m.

现设 A 是元素属于域 F 的 $n > 1$ 阶方阵．如果对于满足 $1 \leqslant r \leqslant n-1$ 的某整数 r，A 不包含一个 $r \times (n-r)$ 型的全零子矩阵，则称 A 是完全不可分的 (fully indecomposable)．所以，$n > 1$ 阶的完全不可分矩阵 A 的全部非零元素不能全含于 A 的 n 个既有行又有列的条中．阶数 $n = 1$ 时，A 为完全不可分的，即 A 不是 1 阶零矩阵．作为定理 6.1 的直接推论可得，一个完全不可分的 $n > 1$ 阶方阵 A 的项秩等于 n，从而 $\det(M) \neq 0$．但是由 $\det(M) \neq$

0 一般并不能推出 A 完全不可分．然而下述定理指出，A 的完全不可分性可以用 det(M) 的一个代数性质来刻划[38]，这一事实在 Frobenius 的工作中已经是明白的了．

定理 6.2. 设 A 是元素属于域 F 的一个 n 阶方阵，设 $M=A*X$ 是与 A 相伴的形式关联矩阵，则 A 完全不可分当且仅当 det(M) 是多项式环 $F^*=F[x_{11}, x_{12}, \cdots, x_{nn}]$ 中的不可约多项式．

在这一节里，我们指出了未定元在组合矩阵论中的两种用法．然而，我们预期会出现许多其它用法，而且，矩阵与未定元相结合将会提供一种处理各类组合问题的非常有效的手段．

参 考 文 献

[1] S. A. Amitsur and J. Levitzki, Minimal identities for algebras, *Proc. Amer. Math. Soc.*, **1** (1950), 449—463.

[2] W. G. Bridges, Some results on λ-designs, *J. Combinatorial Theory*, **8** (1970), 350—360.

[3] ————, The polynomial of a non-regular digraph, *Pacific J. Math.*, **38** (1971), 325—341.

[4] W. G. Bridges and E. S. Kramer, The determination of all λ-designs with λ=3, *J. Combinatorial Theory*, **8** (1970), 343—349.

[5] W. G. Bridges and H. J. Ryser, Combinatorial designs and related systems, *J. Algebra*, **13** (1969), 432—446.

[6] R. A. Brualdi and H. Perfect, Extension of partial diagonals of matrices I, *Monatsh. Math.*, **75** (1971), 385—397.

[7] N. G. de Bruijn and P. Erdös, On a combinatorial problem, *Indag. Math.*, **10** (1948), 421—423.

[8] P. J. Cameron, Biplanes, *Math. Z.*, **131** (1973), 85—101.

[9] P. Dembowski, Finite Geometries, Springer-Verlag, Berlin, 1968.

[10] R. P. Dilworth, A decomposition theorem for partially ordered sets, *Ann. of Math.*, (2) **51** (1950), 161—166.

[11] J. Edmonds, Systems of distinct representatives and linear algebra, *J. Res. Nat. Bur. Standards*, **71B** (1967), 241—245.

[12] L. R. Ford, Jr., and D. R. Fulkerson, Flows in Networks, Princeton University Press, 1962.

[13] J. M. Goethals and J. J. Seidel, Orthogonal matrices with zero diagonal, *Canad. J. Math.*, **19** (1967), 1001—1010.

[14] A. W. Goodman, Set equations, *Amer. Math. Monthly*, **72** (1965), 607—613.

[15] M. Hall, Jr., A problem in partitions, *Bull. Amer. Math. Soc.*, **47** (1941), 804—807.

[16] ————, Distinct representatives of subsets, *Bull. Amer. Math.*

Soc., **54** (1948), 922—926.

[17] ——————, Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.

[18] P. Hall, On representatives of subsets, *J. London Math. Soc.*, **10** (1935), 26—30.

[19] A. J. Hoffman, Research problems, *J. Combinatorial Theory.*, **2** (1967), 393.

[20] A. J. Hoffman and McAndrew, The polynomoal of a directed graph, *Proc. Amer. Math. Soc.*, **16** (1965), 303—309.

[21] W. B. Jurkat and H. J. Ryser, Matrix factorizations of determinants and permanents, *J. Algebra,* **3** (1966), 1—27.

[22] J. B. Kelly, Products of zero-one matrices, *Canad. J. Math.*, **20** (1968), 298—329.

[23] D. E. Knuth, The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, Addison-Wesley, Reading, Mass., 1969.

[24] ——————, Notes on central groupoids, *J. Combinatorial Theory,* **8** (1970), 376—390 .

[25] E. S. Kramer, On λ-designs, Dissertation, University of Michigan, 1969.

[26] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, On the existence of a projective plane of order 10, *J. Combinatorial Theory,* **A14** (1973), 66—78.

[27] M. Marcus and H. Minc. Permanents, *Amer. Math. Monthly.*, **72** (1965), 577—591.

[28] M. Marcus and M. Newman, Inequalities for the permanent function, *Ann. of Math.*, 75 (1962), 47—62.

[29] L. Mirsky, Transversal Theory, Academic Press, New York, 1971.

[30] H. Perfect, Symmetrized form of P. Hall's theorem on distinct representatives, *Quart. J. Math. Oxford Ser.*, (2) **17** (1966), 303—306.

[31] H. J. Ryser, Combinatorial Mathematics, Carus Math. Monograph No. 14, Mathematical Association of America, 1963.(即本书)

[32] ——————, An extension of a theorem of de Bruijn and Erdõs on combinatorial designs, *J. Algebra,* **10** (1968), 246—261.

[33] ——————, Combinatorial configurations, *SIAM J. Appl. Math.*, **17** (1969), 593—602.

[34] ——————, A generalization of the matrix equation $A^2=J$, *Linear Algebra and Appl.*, 3 (1970), 451—460.

[35] ——————, A fundamental matrix equation for finite sets, *Proc. Amer. Math. Soc.*, 34 (1972), 332—336.

[36] ——————, Intersection properties of finite sets, *J. Combinatorial Theory,* **A14** (1973), 79—92.

[37] ——————, Analogs of a theorem of Schur on matrix transformations, *J. Algebra,* **25** (1973), 176—184.

[38] ——————, Indeterminates and incidence matrices, *Linear and Multilinear Algebra,* **1** (1973), 149—157.

[39] J. J. Seidel, Strongly regular graphs with $(-1, 1, 0)$ adjacency matrix having eigenvalue 3, *Linear Algebra and Appl.*, **1** (1968), 281—

298.

[40] R. G. Swan, An application of graph theory to algebra, *Proc. Amer. Math. Soc.*, 14 (1963), 367—373.

[41] ————, Correction to 'An application of graph theory to algebra,' *Proc. Amer. Math. Soc.*, **21** (1969), 379—380.

[42] W. T. Tutte, The factorization of linear graphs, *J. London Math. Soc.*, **22** (1947), 107—111.

[43] D. R. Woodall, Square λ-linked designs, *Proc. London Math. Soc.*, (3) **20** (1970), 669—687.

补充:

[44] H. Minc, Permanents, Encyclopedia of Math. and its Appl. (G. C. Rota ed.), Vol. 6, Addison-Wesley, Reading, Mass., 1978. 对此书的书评刊于*Bull. Amer. Math. Soc. N. S.*, Vol. **1** (1979), 965—973.

[45] H. J. Ryser, Indeterminates and incidence matrices, in Combinatorics, —Proc. of the NATO Advanced Study Institute, 1974. (Ed. M. Hall, Jr., and J. H. Van Lint.)

[46] ————, Matrices and set intersections, *Linear Algebra and Appl.*, **37** (1981), 267—275.